EC における情報セキュリティに関する
活動報告書 2008

平成 21 年 3 月

次世代電子商取引推進協議会

はじめに

ほとんどのユーザーが PC とネット利用に不安感を感じているとの調査結果が、2007 年 9 月にメディアで公開された。内容は「ネットユーザー8 割が、ネット利用中に迷惑行為に遭った経験あり」 というもので、出典はトレンドマイクロ社の「インターネットの利用動向」：迷惑行為実態調査である（18 歳以上一般ユーザー対象にオンラインアンケートを実施、1000 名から回答)。
この調査結果の詳細数字を見てみると 、実に回答者の 82%がネット利用時に迷惑行為を経験しているという前述の内容である。
この他にも、「望まないポップアップメッセージや大量の広告が表示」（30.6%）や 「大量の迷惑メールを受け取り」（26.6%） 、それに「訪問 Web サイトから知らないプログラムがダウンロードの未遂 or 既遂（つまり、やりそうになったもしくはやってしまった)」（12.4%） が、続いており、結果として何と、「ネットや PC 利用時に不安を感じている」のは、ユーザー全体の 98% に達しているという冒頭の調査結果である。
具体的な不安の内訳としては、「知らないうちにウイルスやスパイウェアに感染してしまうのではないか」（25%)、「ネットショッピング等でクレジットカード番号や口座番号入力が不安」（22.8%） 、「PC 不具合となり、写真やメール等の大切な情報を失う恐れ」（18.7%）等であり、オンラインアンケートでの結果（敏感なネットの先進ユーザーが含まれる）であることを考慮しても、このユーザー心理の実態は、これから益々期待される EC（電子商取引）の健全な発展に対して、重大な普及阻害要因になりかねない。また、安全・安心 EC 環境整備の必要性という観点からも、この現状に対して早急に対策をしなければならないことは論を待たない。
そこで、当次世代電子商取引推進協議会の安全・安心 EC 環境整備グループとしては、昨年に引き続き情報セキュリティ・ワーキンググループ（WG）を立ち上げて、その傘下に 4 つの重点テーマ別にサブワーキンググループ（SWG）を設置して、その現状把握と対策検討を目指すことになった。
以下が、その活動結果報告書である。

平成 21 年 3 月

次世代電子商取引推進協議会

目　次

1. 情報セキュリティ WG 全体(全体会議)と SWG 活動概要----------1
1.1. ネット脅威の現状と情報セキュリティ保護の必要性----------1
1.2. 本年度､情報セキュリティ WG(全体会議)と SWG 活動----------2
2. 企業間情報保護連携 SWG 活動報告----------5
2.1.活動概要----------5
2.2.企業間情報保護連携の必要性と問題点----------10
2.3.業務委託に関する事例と企業間情報保護連携の先行事例----------14
2.4.業務データプロセスセキュリティ評価チャートによるアプローチ----------16
2.5.本アプローチによる企業間情報連携の展開----------21
2.6.本アプローチのメリット・デメリット----------25
2.7.おわりに----------30
企業間情報保護連携 SWG(SWG1)メンバーリスト----------34
参考文献・資料----------35
付録 A　平成 20 年度　事業計画----------36
付録 B-1　メンバーへのアンケート資料----------37
付録 B-2　アンケート回答----------45
付録Ｃ　業務データプロセスセキュリティ評価チャート　ワークシート----------48
3. WEB セキュリティ SWG 活動報告----------49
はじめに----------49
3.1.電子商取引と Web セキュリティの現状----------50
3.2.本 WG の活動方針と調査報告----------62
3.3.まとめ----------75
参考文献----------76
関連するサイト一覧（順不同）----------77
Webセキュリティ SWG(SWG2)メンバーリスト----------79
4. ＰＫＩ適正運用・利活用 SWG 活動報告 ----------80
4.1.活動概要----------80
4.2.事例調査----------81
4.3.運用/利用方法の考察----------94
4.4.まとめ----------96
4.5.付録 PKI と SSL----------97
PKI 適正運用・利活用 SWG（SWG3）メンバーリスト----------99
5. データフォレンジック活用策検討SWG活動報告----------100
5.1.活動概要----------100
5.2.EC(電子商取引)の観点からみたデジタル・フォレンジック有効性----------107
5.3.EC（電子商取引）におけるデジタル・フォレンジックの適用課題----------109
5.4.各種フォレンジック関連ガイドラインの紹介----------110

5.5.デジタル・フォレンジック・マネジメント態勢構築支援サービス----------112
データフォレンジック活用策検討 SWG（SWG4）メンバーリスト ----------114
参照及び引用文献と参照及び引用サイト一覧----------115
6. おわりに----------116

1. 情報セキュリティ WG（全体会議）と SWG 活動概要

1.1 ネット脅威の現状と情報セキュリティ保護の必要性

1.1.1. ネット脅威の現状

まず、近年の傾向として顕著なものは、そのリスクなり脅威が、一般には目立たないように、つまりユーザー自身が、簡単には気がつかないものとなってきている事が挙げられる。
この「目立たない化」（ステルス化）現象は、今まで攻撃者が無差別・無作為に大量のアタックを仕掛けていたのに対して、次第に特定のターゲットの的を絞り、様々なステルス手段で確実に経済的利益を得る仕掛けに、大きく方針変更した結果だと思われる。
その代表的攻撃（アタック）事例としては下記の通りである。

- ボット攻撃を受けると、従来のウイルスと違って感染しても症状が表に出ない、ユーザーが感染そのものに気付かないのが特徴である。つまり、メールの添付ファイルをうっかり開封すると、本文リンクによりボットが埋込まれ、悪質サイトへ誘導される仕組みである。
- 感染 PC をボットネット制御するマルウェア「Storm Worm」が猛威を振るう
  その時期のタイムリーな注目ニュースや季節行事に便乗、出会い系やゲーム、会員登録、e カード写真のダウンロード等によりボットのネットワークに感染する。この場合、背後に犯罪組織があることが多く、知らないうちに大規模な DDoS 攻撃に参加させられるというものである。
- 正規のサイトさえも危ない、つまり攻撃手段が迷惑メール（スパム）を使ってのものから、脆弱性を持った Web 攻撃へと移行している。このため、Web サイトにアクセスするという日常的行為の裏で、ユーザーが気付かず感染しているケースが多々ある 。

この Web サイトへの攻撃は厄介である。当然、プログラムは通常 HTTP 通信でダウンロードされるためその中に悪意のマルウェアが入っていても検出困難であり、基本的な通信窓口である 80 番ポートは閉じられないという基本的な状況がある。
この Web を介した脅威を数量的に見ても、毎年急増している、例えば 2007 年初めの件数は 2004 年末時点の約 5 倍増加（トレンドマイクロ調べ）という分析結果も出ている。
こういった急激な増加理由の 1 つには、「Mpack」というマルウェアパッケージの存在がある。これは、Web サイトにアクセスする PC に攻撃用コードを送り込むマルウェアの作成ツールである。これが、簡単にネット上で誰にでも、有料ダウンロードできるネット環境になっているのが大きな問題である。
さらには、サイト閲覧時に即感染したり、複数アプリ脆弱性を悪用する不正プログラムのサービス提供やボット対策ツールを逆検出してこれから逃れる忌避機能等の拡張用のコンポーネントを追加ダウンロードさせる、サービスとしてのエクスプロイト業界（exploits as a service）」が活況を呈している。このサービスは SaaS ならぬ「EaaS」と呼ばれて流行しているにいたっては、何をかいわんやの状況である。
また、最近は「SEO（Google）ポイズニング」と呼ばれる Web 検索を悪用して、トロイの木馬等を感染させる攻撃も登場している。これは、Google や Yahoo!等有力な検索エンジンに特定の

サービスキーワード（例えば、Happy Christmas）をインプットして検索にかけると、その結果表示の検索インデックスページ上位には、ズラッと悪質サイトが表示されるというものである。

こういった､悪意を持った攻撃の多様化は止まるところを知らず､いわゆるサイバー犯罪自体が、愉快犯的なものから、完全に営利目的に移行しており、しかも標的の中心は金融機関だけではない状況になってきている。
特に、米国では市場規模年間約 100 億ドルというオンラインゲームは、攻撃者に“おいしい”市場となっており、ユーザーアカウント情報を盗めば、関連したキャラクターのレアアイテムや現金をオークションサイトや Web ストアで売買可能で、マネーロンダリングの対象になっている。ある調査によると、新発見悪意コード上位 50 種のうち 5%が、このオンラインゲームのアカウント情報を攻撃対象となっている現実がある。
さらに最近は、テキストデータのフィルタ回避のための静止画像スパム（宣伝文句を画像ファイルに）の代わりに、正規 CM やニュース番組の動画を利用するものまで登場し、新たに PDF 利用して株価操作（偽情報で吊り上げ､売り抜け）やウイルス感染を狙うスパムまで登場している。
また、2008 年のセキュリティ脅威の傾向としては、Web の脅威がさらに増大、すでにガジェットが攻撃に利用ケースもあり、RSS や マッシュアップといった Web2.0 技術を悪用した「トロイの木馬 2.0」等マルウェア攻撃が、始まっており、これまで非対象であった Mac やスマートフォン等モバイル機器等、Web 利用攻撃のクロスプラットフォーム化が進行している。

1.2. 本年度､情報セキュリティ WG 全体（全体会議）と SWG 活動

このような状況を受けて、本年度は前述のように昨年度に続き、安全・安心な EC 推進グループ活動の一環として、この情報セキュリティ WG（全体会議）を組織し、傘下に 4 つのサブワーキング（SWG）を設置して、各々に活動テーマ（下記）掲げて推進した。
以下、情報セキュリティ WG の活動、すなわち 4 つの SWG のテーマ検討＆推進結果を報告する全体会議の概要を記載し、現在の電子商取引が抱える一大課題としての情報セキュリティ保護レベルの向上により、さらなる電子商取引発展の一助となるべく、この成果報告書を作成する。
本年度の当情報セキュリティ WG（ワーキンググループ）の編成であるが、WG 全体会議の傘下に 4 つの SWG（サブワーキング）を設置して、各リーダを選任して各々の研究テーマを推進した。
また各 SWG のテーマに関連して、今回の報告書で取り上げる「情報セキュリティ」と「電子商取引（EC）」の関係であるが、大きく分けて EC の形態によって、やはり B to B と B to C の 2 つの「情報セキュリティ」分類に大別できる。
まず B to B の情報セキュリティとしての課題の 1 つは､企業間における情報共有に起因するものである。例えば、共同開発における企業秘密の保護に関する課題や関連企業への業務委託、それに専門企業へのアウトソーシングに付随するもの等が上げられる。
特に、近年は個人情報保護の高まりによって、委託元企業における委託先企業に対する安全な情報管理の監督責任を問われるケースについて、それに関連した法制度やガイドラインの整備によりさらに注目されている。

この課題については今年度の当協議会、安全安心グループの活動の一環として、情報セキュリティ WG 全体の取り組みの中で、「企業間情報保護連携ガイド策定・利用促進（SWG1)」のサブワーキングテーマとして取り組むことにした。
また B to C の課題としては、やはりインターネットの環境整備によって、電子商取引を誰もが利用できる環境が整備されてきた一方で、インターネットに潜む、ボット、ウイルス、フィッシングなどのリスクが顕在化してきている。電子商取引が普及すればするほど、つまりプレーヤー（商取引当事者）が、IT リテラシーのある大人から平均的社会人・子供・老人へと拡大すればするほど、リスクは肥大化する傾向にあることはいうまでもない。その多様化に伴い、ヒューマンインタフェースとして消費者が接する、Web 関連の安全性について検討していく必要があると判断した。
この課題については、昨今の悪意ある攻撃者からのアタック手段が、メールから Web に移行していることを踏まえた上で、サイト運営者への注意喚起も含めて「Web セキュリティ課題検討・普及啓発（SWG2)」のテーマとして取り組むことにした。
次に、電子商取引としてのインフラを考えた場合に、それが B to B と B to C の商取引形態の如何に係わらず、信用取引の基本として PKI（「公開鍵暗号基盤」）があることはいうまでもない。この公開鍵暗号方式を利用したセキュリティインフラについては、SSL（Secure Sockets Layer：セキュアソケットレイヤー）等として広く普及していることは周知の通りであるが、また様々な課題があることも事実である。
この課題検討については、認証局や証明書等の運営・発行や Web サイトでの表示の仕方等について問題点を検証するために、「PKI 適正運用・利活用の促進（SWG3)」のテーマとして取り組むことにした。
続いて、電子商取引としてのセキュリティを考えた場合、何かのトラブル発生で取引相手から訴えられた時の対応を準備する必要があると考えている。例えば B to B であれば発注元企業と受注先企業の間で注文数に違いがあるケース、また B to C であれば、消費者の注文数と Web サイトの受注数に違いがあるケースなどである。また、訴訟対応という点では、企業内部で情報漏えいが発生した場合に、その安全管理責任を問われるケース等が想定できる。
この課題検討については、デジタル・フォレンジックという観点から、様々な電子証跡を残すにはどうしたよいのかという点で、「データフォレンジック活用策検討（SWG4)」のテーマとして取り組むことにした。

1.2.1. 活動体制（情報セキュリティ WG 傘下）と各 SWG の将来にわたる具体的検討テーマ案

（本年度はこれらの中から、テーマを絞って取り組むこととする。）

1. 企業間情報保護連携ガイド策定・利用促進テーマ（SWG1）

①EC 関連の個人情報委託に関する契約注意事項
②機密情報アウトソーシング時の情報セキュリティ保護ポイント
③預託企業・受託企業（中小企業）の情報セキュリティガイド

2. WEB セキュリティ課題検討・普及啓発テーマ（SWG2）

①EC 関連の Web セキュリティ全般検討
②EC サイト構築時の情報セキュリティ注意事項

③Web サイト運営者向けの情報セキュリティ検討事項
④中小（企業）サイト向け Web 対策含む情報セキュリティガイド
⑤Web サイトセキュリティ注意事項まとめ（消費者向け）

3. PKI 適正運用・利活用の促進テーマ（SWG3）

①認証局脆弱性の検証と注意喚起事項
②企業側 PKI 運用時の適正化検討内容
③信用できるサイト認証のためのユーザーガイド
④EC 関連のネットワークセキュリティや決済端末関連の脆弱性検討

4. データフォレンジック活用策検討テーマ（SWG4）

①EC 関連のコンピュータ・フォレンジック適用全般検討
②EC サイト運営時のフォレンジック注意事項
③J-SOX 対応の EC フォレンジック検討事項
④フォレンジック・ツール導入時のユーザーガイド

1.2.2. 情報セキュリティ WG（全体会議）活動経過

表 1-1 情報セキュリティ WG（全体会議）の活動経過

期日	活動内容
平成 20 年 6 月 13 日	第 1 回情報セキュリティ WG（全体会議）
	・メンバー紹介 ・基調講演：経済産業省における情報セキュリティ政策 （情報セキュリティ政策室：清水課長補佐） ・WG の活動概要、スケジュール、SWG 活動について
同年 9 月 15 日	第 2 回情報セキュリティ WG
	・有識者講演：「シマンテック：グローバルセキュリティレポート」： 最新インターネットセキュリティ脅威：マリシャスコード等について （講師）テルミ・ラスカウスキー執行役員（日本・香港地域担当） ・各 SWG の事例調査と中間報告(目次、纏め方)について
同年 11 月 26 日	第 3 回情報セキュリティ WG
	・有識者講演：マイクロソフト社情報セキュリティ取り組み （業務委託先の個人情報保護とセキュリティ保護システム） （講師）マイクロソフト社：小川部長 ・SWG 活動報告と成果報告(案)について
平成 21 年 2 月 6 日	第 4 回情報セキュリティ WG
	・今年度情報セキュリティ WG 活動成果報告書（案）の確認 ・SWG 活動報告トピックスと来年度活動案について

2. 企業間情報保護連携 SWG 活動報告

はじめに

日本の情報セキュリティ向上の活動は、2000 年以降にインターネットによる情報流通、電子商取引が急速に普及する中で、盛んにおこなわれてきた。2007 年には電子商取引額は企業間（B to B-EC）で 162 兆円、消費者企業間（B to C-EC）で 5 兆円に及んでいる。この間、情報セキュリティ犯罪は、情報を盗み出したなどを告知して自分の技術を誇示するという愉快犯から、インターネット上で情報を共有して経済的な犯罪を行なう経済犯に変貌してきているのである。

現在、インターネット上には、セキュリティホールを探す情報、そのセキュリティホールから情報を盗み出すためのやり方をアナウンスする情報、そのアナウンスによって情報を盗み出し情報を販売する情報があり、その情報を使って個人や企業からお金を搾取するものがインターネット上でそれらの情報をやり取りし、巧妙に情報を共有して攻撃してきている。これに対し、個人情報保護対策や情報セキュリティ対策は、企業や組織毎の対策を中心に進めてきている。不特定多数の情報を巧妙に共有した攻撃に対し、企業や組織毎の対策では限界があると感じた。

そこで、企業と企業、組織と組織での情報を利活用する上で、企業間での情報保護連携を如何にすべきであるかということを検討するために、本年度から、新たに「企業間情報保護連携ガイド策定・利用促進」事業を開始し、情報セキュリティ WG の配下に企業間情報保護連携 SWG を組織し、ECOM 自主活動を行なうこととした。

2.1. 活動概要

2.1.1. 活動目的

我が国の政府は世界最高水準のセキュリティ国家を目指し、政府、業界団体、民間において様々な取り組みを積極的に推進してきている 。情報セキュリティマネージメントシステム ISMS（Information Security Management System）を中心とした企業情報システムのセキュリティ管理の取り組みである。その中には、企業の情報システムのセキュリティ管理の認定制度や監査制度などがあり、業界団体、民間企業と連携しながら進めている。

一方、1990 年代に欧州などから要求されたプライバシー保護（EU 指令）により、日本でも個人情報法が 2005 年 4 月に制定された。法律の制定に伴い、政府、業界団体、民間企業は個人情報保護に関する様々なガイドラインや認定制度が作成している。これらの取り組みでも、企業（事業者）毎の個人情報の取り扱いを規定し、企業単位での行動指針やシステム評価をする取り組みである。

これらの情報セキュリティ対策やプライバシー保護の取り組みが高度化すればするほど、顧客情報の収集、商品やサービスの案内、配送、決済業務を行う現場では厳しい制約（守るべき規定）が課せられるようになる。制約が高度化し、複雑かつ厳しくなると、できること、できないことが現れてくる。また、それぞれの業務で本来守るべき規則までもが形骸化し、忘れ去られる。

情報セキュリティ対策や個人情報保護対策にガイドラインや統一基準を設け、守れるように対策を低いレベルに合わせていくと、経済犯の付け入るすきを与えてしまう。逆に、企業単位で情報セキュリティを評価する取り組みでは、高いセキュリティレベルを取得した企業が愉快犯からの格好の標的となる。統一基準や企業単位でのセキュリティ評価は、愉快犯や経済犯に格好の材料を与えることになるのである。

企業単位での取り組みが高度化すればするほど、戦略的かつ積極的にセキュリティ対策が行われるレベルを超え、情報を利活用して業務を実施している現場では「もういいよ」という意識が生まれる。従来の企業ごとに行なう取り組みによる情報セキュリティ対策や個人情報保護を進めていくことは限界に来ている。電子商取引を行う者たちが、戦略的かつ積極的に行える実行性能のある対策や保護を実現する仕組みが必要である。

上記の問題意識から、本年度は情報セキュリティ WG の配下に企業間情報保護連携 SWG（以下 SWG1 と呼ぶ）を置き、電子商取引を行う企業間でどのような情報保護連携が必要であるか、戦略的かつ積極的に実行性能のある新しい取り組みとは何か、それによって、中小企業も含めた企業間での情報共有における情報セキュリティをどのように向上させればよいかの検討を行った。

企業間情報保護連携の初年度の取り組みとしては、平成 20 年 3 月に改定された個人情報保護のガイドラインに含まれる業務委託を行う際の「委託先の適切選定、必要な契約の締結、取扱状況の把握」をテーマとし、企業間情報保護連携のあるべき姿についての以下の活動を行った。

（1）企業間で情報保護の連携を必要とする対象と検討スコープの設定
（2）企業間情報保護連携の問題点と共通課題の醸成
（3）共通認識された課題に対する解決のアプローチの策定

2.1.2. 活動経過

本事業は、平成 21 年度 ECOM 自主活動として、情報セキュリティ WG の配下に、15 の企業・団体の会員メンバー11 名、有識者 6 名、オブザーバー2 名、事務局 2 名から構成される企業間情報保護連携 SWG(以下では SWG1 と呼ぶ)を組織した。4 回のワーキンググループ（WG）全体会議への参画と 4 回の SWG によるテーマ別検討を行った。なお、当初、SWG1 への参加者が少なかったため、SWG2 メンバーや有識者の協力を得て、SWG１を運営した。

本事業は、業務委託における委託先の適切な選択や適切な監督の際の評価項目を事務局が提案し、メンバーからの意見により必要最低限の評価項目や理想とする評価項目を検討し、企業間での守るべき基準をガイドとしてまとめる事業計画であった[付録 A]。

（1）活動計画の見直し

第 1 回 WG で、参加メンバーより、必要最低限の評価項目や理想とする評価項目を集めることは、①統一的な基準を作る従来活動と同じになってしまうこと、②集まったメンバーの分野や問題意識が異なること、③企業が使っている項目を開示することが困難なことから、具体的な活動内容を変更した。

第 1 回 SWG では、企業間情報保護連携の対象とする情報、連携の仕方、必要とするセキュリティレベルの範囲を設定した。

8 月に参加メンバーによる企業間での業務委託に関する事例収集を行い、第 2 回の SWG に集まった 8 事例により課題を検討し、活動することとした。

（2）参加メンバーによる事例の収集と共通課題の検討

第 2 回 SWG では、企業間情報保護連携の対象情報、連携形態、セキュリティレベルのスコープを整理していくとともに、収集した 8 事例をベースとして、想定課題を検討した。その結果、企業間での業務委託では、委託する業務内容、取り扱う情報が必要とする情報保護の基準は、千差万別であり、共通した基準や評価の項目では十分カバーできない。そこで、戦略的かつ積極的に行える実行性能のある対策や保護を実現する仕組みがどうすれば実現できるかを中心に検討を進めた。

（3）解決のアプローチの検討

収集した 8 事例の中に、委託先との契約に際し、委託元と委託先の業務プロセスと個人情報保持すべき情報のフロー図を作成して明確化し、そのフロー図を契約書に添付して適正な契約と監督を行っている先行事例があり、第 3 回 WG でその取り組みを他のメンバーと共有した。

第 3 回 SWG では、紹介を受けた事例をベースとして、事務局が自ら行なう行事を例題として、機密保持すべき情報のフロー図を作成して、委託先の選定、契約、監督を行う際に、注意すべきポイントが明確となることを提案した。その例題を用いて、企業間での情報保護の合意形成の手順やフロー図の記述内容・表記方法に関して、参加メンバーと検討した。

（4）成果の纏め

12 月にフロー図の表記方法、記述内容に関してメンバーにアンケートを取り、第 4 回の SWG でメリット、デメリットについて検討し、企業間情報ほど連携における解決のアプローチとして活動成果を纏めた。事務局にて活動内容と成果を報告書に纏め、第 4 回の WG にて、活動報告内容を承認いただくとともに、本活動のアプローチを ECOM スタイルとすることを提案した。

企業間情報保護 SWG（SWG1）およびそれに関連する活動の経過を表 2-1 示す

表 2-1　SWG1 等の開催経過

期日	活動内容
平成 20 年 6 月 13 日	第 1 回情報セキュリティ WG
	・本年度の活動計画原案の提案（事務局）
7 月 15 日	第 1 回企業間情報保護連携 SWG
	・企業間での情報共有で情報保護の連携を必要とする対象と課題 ・個人情報保護ガイドラインの改定(2 月末)の情報セキュリティ対策
8 月	メンバーによる事例収集（8 事例）
9 月 11 日	第 2 回企業間情報保護連携 SWG
	・事例調査について ・討議 　－企業間で情報保護の連携を必要とする対象と課題 　－個人情報保護ガイドラインの改定の情報セキュリティ対策 ・今年度の報告内容と今後の予定について
9 月 29 日	第 2 回情報セキュリティ WG（活動の方向性の確認）
11 月 6 日	第 3 回企業間情報保護連携 SWG（SWG メンバー約 10 名参加）
	・これまでの活動の整理 　－企業間で情報保護の連携を必要とする対象と課題 　－個人情報保護ガイドラインの改定の情報セキュリティ対策等 ・委託業務における情報保護の共通認識を得るチャートの紹介 ・今後の活動内容の提案と今年度の報告内容について ・今後の予定
11 月 26 日	第 3 回情報セキュリティ WG
	・先行事例（マイクロソフト）の紹介（WG メンバー約 30 名参加）
12 月 5 日	ECOM 中間報告会（企画部会、安全・安心 EC 環境整備委員会）
12 月	業務データプロセスセキュリティ評価チャート アンケート
1 月 23 日	第 4 回企業間情報保護連携 SWG
	・提案方式のメリット・デメリット等の討議 ・報告内容レビュー
2 月 4 日	第 35 回 ECOM セミナー
	・先行事例（マイクロソフト）の紹介（ECOM 会員　約 100 名）
2 月 6 日	第 3 回情報セキュリティ WG
	・報告内容の確認

2.1.3. 活動成果

初年度の活動として、個人情報の保護に関する法律についての経済産業分野を対象とするガイ

ドラインの改正における「委託先の適切選定、必要な契約の締結、取扱状況の把握」を例として、企業間情報保護連携の課題と解決のアプローチを得た。企業間情報保護連携 SWG の初年度の活動成果は下記のとおりである。

（1）企業間情報保護連携の検討対象

企業間情報保護連携活動を行なう初年度として、の検討を行うスコープ（検討対象）を設定した。

■対象情報のスコープ　＜初年度の検討対象

・情報の種類（人、物、金）　＜個人情報
・秘匿性（厳秘、(秘)、関係者外秘、開示、公開）　＜関係者
・取り扱い（期間、アクセス回数、アクセス人数）　＜有期、多アクセス、数名

■情報共有の形態

・関係者数（1 対 1、1 対 N、N 対 M、N 対 N）　＜1 対 1（企業間）
・関係（対等、上下、委託）　＜委託関係

（2）企業間情報保護連携の課題

委託業務において、委託する範囲、取り扱う情報が千差万別であり、共通した基準やセキュリティ対策や評価も千差万別である。共通した評価基準を作ることは困難であり、業務に携わる関係者間での共通認識と合意形成が重要であることに気付いた。

■共通した情報保護基準作成の困難性
■委託契約事項（情報保護要件）の具体性の欠如
■業務に携わる関係者間での共通理解・共通認識の重要性

（3）解決アプローチの作成

先行事例や参加メンバーや有識者の指摘により、業務データプロセスセキュリティ評価チャート（Business Data & Process Security Evaluation Chart）による関係者間での情報対策の共通認識方法を作成した。

■業務データプロセスセキュリティチャート（BDPSEC）による解決アプローチ
■データプロセスセキュリティ評価モデルの作成
■標準化した場合の利用シーンと想定効果の検討

なお、本アプローチは、従来の企業ごとに共通した個人情報保護や情報セキュリティの共通した基準を作るというものではなく、案件ごとに関係者間で責任分解点を共通認識ができる図表を作成し、案件に応じた効果的な対策を関係者間で共有しようというものである。

以降では、本活動で得られた企業間情報保護連携の必要性と課題、具体的な解決のアプローチについて、詳細に報告する。

2.2. 企業間情報保護連携の必要性と問題点

本節では、SWG1 で取り扱う電子商取引における企業間情報保護連携の検討対象の範囲について述べ、本事業の契機となった個人情報保護ガイドラインの改正と企業間情報保護連携の必要性とその問題点について報告する。

2.2.1. 情報保護連携の対象

企業間で情報を活用し、その情報の保護対策を考える上では、①情報の種類、②必要とされる秘匿性、③利用期間（保管期間）、利用回数などの情報の取扱という 3 つの視点が考えられる。その 3 つの視点（図 2.1）で、本事業で取り扱う企業間情報保護連携のスコープを検討することとした。

（1）EC を行う上で共有する情報

電子商取引で取り扱われる情報の種類には人、物、金に情報がある。人に関するものとしては、従業員情報、顧客情報など、物の情報としては製品の仕様情報、金の情報としては、製品の価格情報や企業の経営情報など様々である。それらの情報の秘匿性も、公開してよい情報（公開情報）から、取り扱う責任者でも見てはいけない秘匿性を必要とする情報がある。さらに、長く保管し多数の人間で繰り返し利用（アクセス）する情報から、1 回だけ利用し不要になれば破棄できる情報もある。

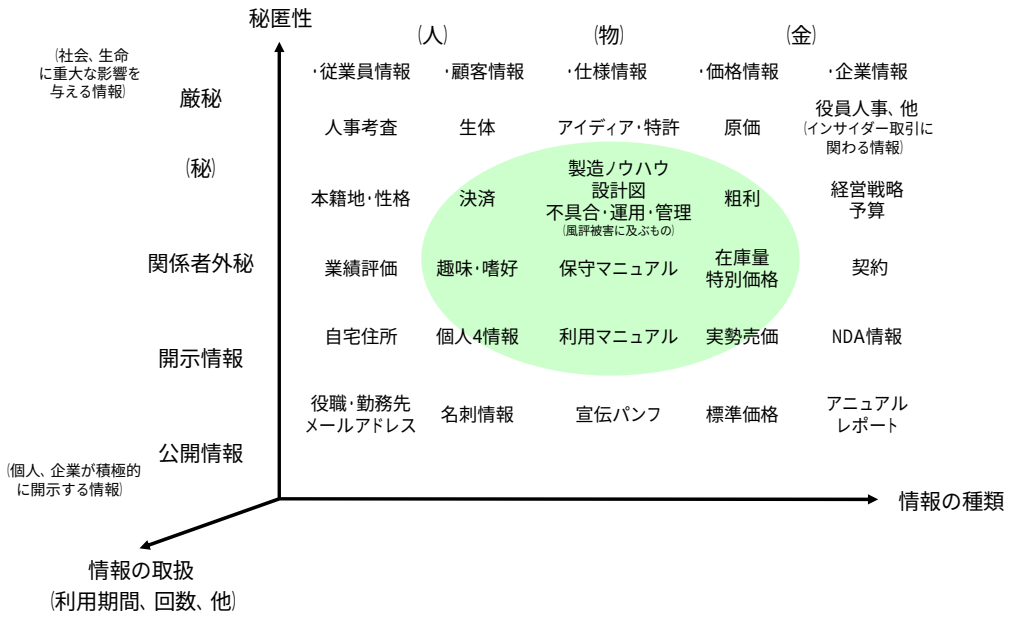


図 2.1 EC を行う上で共有する情報

（2）情報保護対策のレベル

これらの様々な情報が様々な取り扱いをされる業務で、情報保護対策のレベルを考察すると、当たり前であるが、秘匿性が高い情報を長期関に様々な人の間で取り扱う業務では、高いレベルの情報保護対策が必要である。

オンラインショッピング、月例セミナー、フォーラムなどの業務を例に取り考えてみると、図 2.2 に示すように情報保護対策が異なる。特定の業務を想定すれば、そこで取り扱われる情報の種類により、情報保護対策の必要性は決定できる。金融関係を中心として数多くの取り扱い基準がある。オンラインショッピングの広がりとともに、様々なサービス会社がクレジットカード情報を長期にわたり保管し業務に利用するようになり、クレジットカード情報を扱う全ての事業者を対象としたクレジットカード情報保護を目的とした情報セキュリティ基準 PCI DSS（Payment Card Industry Data Security Standard）[2.2～2.3.]のなどが定められている。

初年度の活動としては、PCI DSS のように特定の情報に関する情報保護要件を纏めるというものではなく、企業間で秘匿性を必要とする情報資産をやり取りし、サービスを提供していく企業間の業務データとプロセスを対象とした。

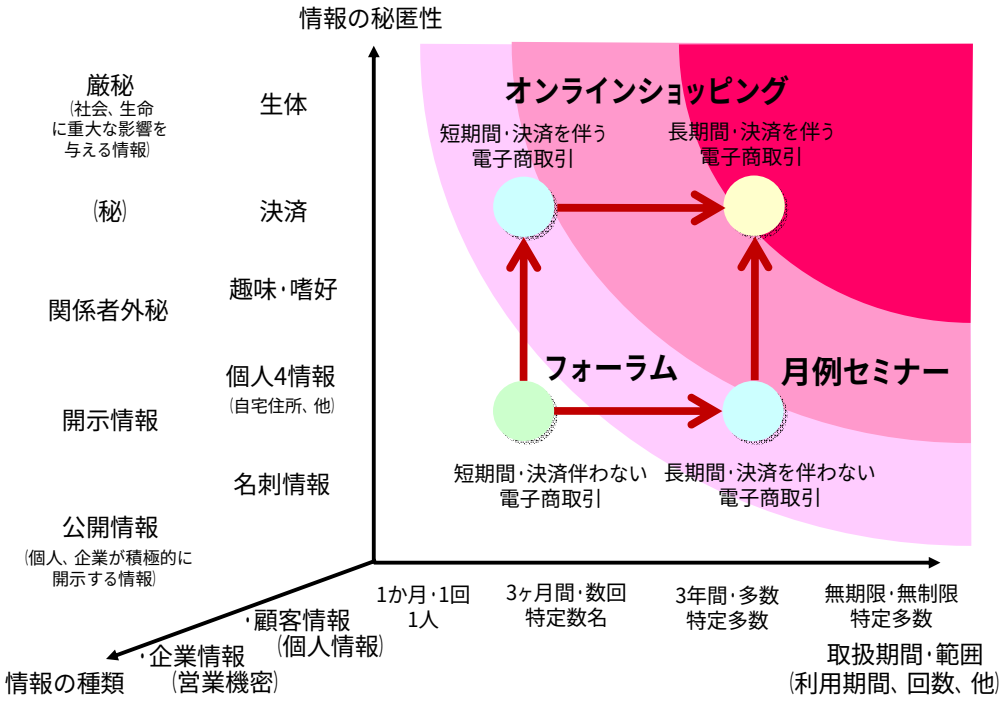


図 2.2　情報保護対策のレベル

（3）情報共有の仕方

今日の情報社会では、多くの事業者がインターネットを介し、情報を共有し、製品やサービスを企業間で連携して提供している。企業や組織間で業務（作業）を分担し、その作業を円滑にこなすために情報を共有する。企業や組織間で情報共有する形態には図 2.3 に示すような様々な関係がある。

初年度の活動としては、1 対 1 の組織間で委託関係を有する情報共有の検討を行なうこととした。

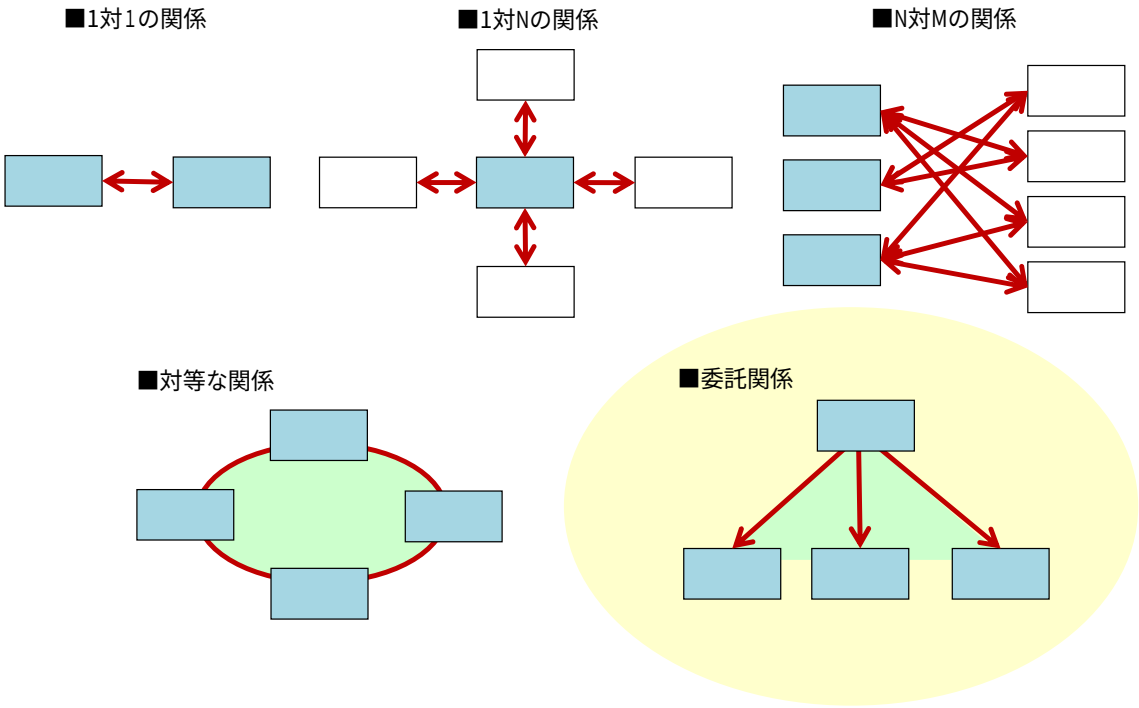


図 2.3 情報共有の仕方

2.2.2. 企業間情報保護連携の方向性

こうした様々な情報、それを取り扱う様々な業務、そして、作業を分担して行なう企業間の様々な関係に対し、従来の個人情報保護や情報セキュリティ対策では機密性、完全性に関する企業単位での守るべき統一基準や評価基準が多い。情報セキュリティ対策や個人情報保護の取り組みが高度化すればするほど、電子商取引で顧客情報の収集、商品やサービスの案内、配送、決済を行う業務に厳しい制約（守るべき規則）が課せられるようになる。制約が高度化し、複雑かつ厳しくなると、作業を行う現場では、本来守るべき規則までもが形骸化するのである。

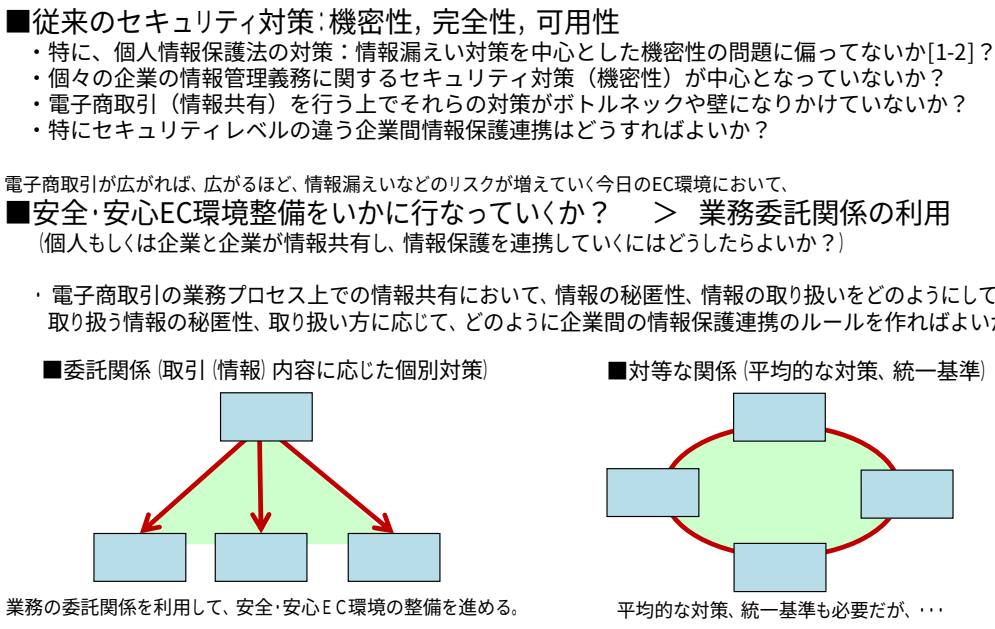


図 2.4 企業間情報保護連携の方向性

図 2.4 に安全・安心な EC 環境を整備していく上で必要となる企業間情報保護連携の方向性を示す。従来の取り組みでは、企業間での可用性（利活用）よりも機密性、完全性が重視されがちである。アウトソーシングとセキュリティ対応[図 2.4～図 2.6]の中でも、機密性、完全性が重視されがちであることが指摘されている。

電子商取引が広がれば、広がるほど、情報漏えいなどのリスクが増えていく今日の EC 環境において、安全･安心 EC 環境整備をいかに行なっていくか？という ECOM の主要課題に対して、電子商取引が広がれば、広がるほど、安全・安心 EC 環境が整備されていくために、業務委託関係の利用し、企業間の情報保護連携を進めていく。業務プロセス上での情報共有において、取り扱う情報の秘匿性、取り扱い方に応じて、どのように企業間の情報保護連携のルールを作ればよいか？を検討していくこととした。

2.2.3. 個人情報保護ガイドラインの改定について

平成 20 年 2 月に個人情報の保護に関する法律についての経済産業分野を対象とするガイドラインの改正－委託先の監督（法第 22 条関連）が交付された。下図に個人情報保護ガイドラインの改定[図 2.5]を示す。委託先の監督に関する改定のポイントは、①委託先を適切に選定すること、②受託者との間で必要な契約を締結すること、③受託者における委託された個人データの取扱状況を把握すること、というものである。

この改定は、これまで自社の業務や情報システムのセキュリティ対策の範囲として検討してきた企業にとっては、委託先の選定、委託先との契約、委託先の取扱状況の把握という他社の業務や情報システムでの取り扱い状況にまで検討範囲が広がったことになる。

〔1〕ガイドラインの改定 〔2-2-3-4.委託先の監督＜法第22条＞〕
個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。
個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合、法第20条に基づく安全管理措置を遵守させるよう、委託を受けた者に対し必要かつ適切な監督をしなければならない〔2-1-4.「＊電話帳、カーナビゲーションシステム等の取扱いについて」の場合を除く。〕。その際、委託する業務内容に対して必要のない個人データを提供しないようにすることは当然のこととして、取扱いを委託する個人データの内容を踏まえ、本人の個人データが漏えい、滅失又はき損等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の性質及び個人データの取扱状況等に起因するリスクに応じた、必要かつ適切な措置を講じるものとする。
「必要かつ適切な監督」には、委託先を適切に選定すること、委託先に法第20条に基づく安全管理措置を遵守させるために必要な契約を締結すること、委託先における委託された個人データの取扱状況を把握することが含まれる。
委託先を適切に選定するためには、委託先において実施される個人データの安全管理措置が、委託する当該業務内容に応じて、少なくとも法第20条で求められる安全管理措置と同等であることを、合理的に確認することが望ましい。また、委託先の評価は適宜実施することが望ましい。
委託契約には、当該個人データの取扱いに関する、必要かつ適切な安全管理措置として、委託元、委託先双方が同意した内容とともに、委託先における委託された個人データの取扱状況を合理的に把握することを盛り込むことが望ましい。
なお、本人からの損害賠償請求に係る責務を、安全管理措置に係る責任分担を無視して一方的に委託先に課すなど、優越的地位にある者が委託元の場合、委託先に不当な負担を課すことがあってはならない。
委託先における委託された個人データの取扱状況を把握するためには、委託契約で盛り込んだ内容の実施の程度を相互に確認することが望ましい。
また、委託元が委託先について「必要かつ適切な監督」を行っていない場合で、委託先が再委託をした際に、再委託先が適切といえない取扱いを行ったことにより、何らかの問題が生じたときは、元の委託元がその責めを負うことがあり得るので、再委託する場合は注意を要する。
なお、漏えいした場合に二次被害が発生する可能性が高い個人データ（例えば、クレジットカード情報（カード番号、有効期限等）を含む個人データ等）の取扱いを委託する場合は、より高い水準において「必要かつ適切な監督」を行うことが望ましい。
[委託を受けた者に対して必要かつ適切な監督を行っていない場合]
事例1）個人データの安全管理措置の状況を契約締結時及びそれ以後も適宜把握せず外部の事業者に委託した場合で、委託先が個人データを漏えいした場合
事例2）個人データの取扱いに関して定めた安全管理措置の内容を委託先に指示せず、結果、委託先が個人データを漏えいした場合
事例3）再委託の条件に関する指示を委託先に行わず、かつ委託先の個人データの取扱状況の確認を怠り、委託先が個人データの処理を再委託し、結果、再委託先が個人データを漏えいした場合
事例4）契約の中に、委託元は委託先による再委託の実施状況を把握することが盛り込まれているにもかかわらず、委託先に対して再委託に関する報告を求めるなどの必要な措置を行わなかった結果、委託元の認知しない再委託が行われ、その再委託先が個人データを漏えいした場合
[個人データの取扱いを委託する場合に契約に盛り込むことが望まれる事項]
・委託元及び委託先の責任の明確化
・個人データの安全管理に関する事項
・個人データの漏えい防止、盗用禁止に関する事項
・委託契約範囲外の加工、利用の禁止
・委託契約範囲外の複写、複製の禁止
・委託契約期間
・委託契約終了後の個人データの返還・消去・廃棄に関する事項
・再委託に関する事項
・再委託を行うに当たっての委託元への文書による報告
・個人データの取扱状況に関する委託元への報告の内容及び頻度
・契約内容が遵守されていることの確認（例えば、情報セキュリティ監査なども含まれる。）
・契約内容が遵守されなかった場合の措置
・セキュリティ事件・事故が発生した場合の報告・連絡に関する事項

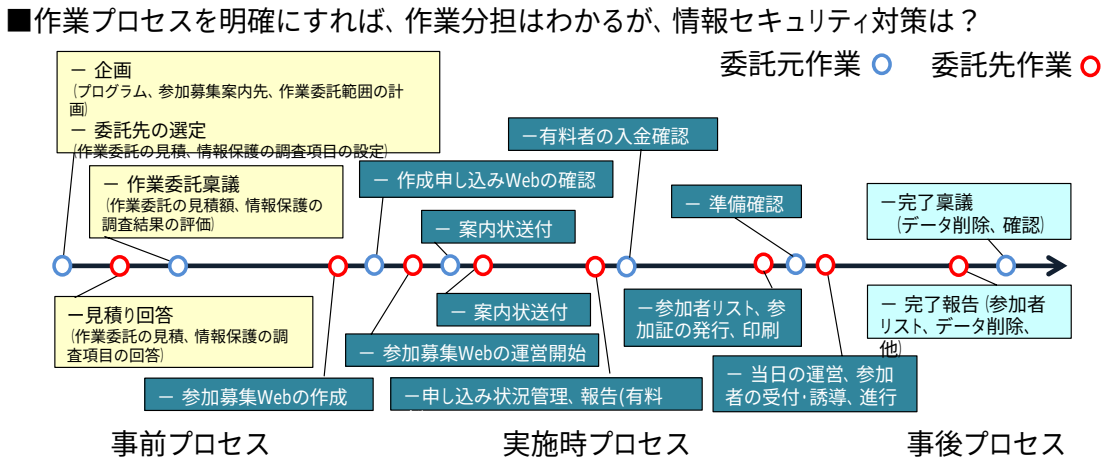
図 2.5 個人情報保護ガイドラインの改定

2.3. 業務委託に関する事例と企業間情報保護連携の先行事例

企業間情報保護連携を検討していくに当たり、業務プロセス上での情報共有において、取り扱う情報の秘匿性、取り扱い方に応じて、どのように企業間の情報保護連携のルールを作ればよいか？を検討していく上で、個人情報保護ガイドラインの改定、特に業務委託に関する改定は具体的な検討テーマである。

（1）事例の収集

そこで、図 2.6 の事例収集の課題を基に、公開されている取り組みや社内外の取り組みに関する事例を参加メンバーとともに収集した。



■いろんな業務に合わせて、様々な基準・規格を作るのか？

・事前　　：業務分担に応じて、どういう項目を評価すべきか？
・実施時　：業務分担に応じて、どういう履歴を残すべきか？
・事後　　：情報漏えいがなかったことをどう報告するか？
・企業間情報保護連携をする上で、見積、契約、仕掛けはどうあるべきか？
・ガイドラインの改正に適合するか？ 例となるか？　秘匿性の高い情報を扱う場合は、永続的に組織で使う場合は？

「委託先の適切選定、必要な契約の締結、取扱状況の把握」の具体的な施策は？？？

図 2.6 事例収集の課題

（2）収集事例と問題点

参加メンバーとともに収集した事例の概要を図 2.7 に示す。

8 事例を収集したが、調査事例 6 を除き、具体的な施策ではなく、問題点を提起するものであった。図 2.8 の収集した事例の位置付けを示す。個人情報保護ガイドラインの改正の「委託先の適切選定、必要な契約の締結、取扱状況の把握」 に対して、業務委託をどうすればいか？、委託先での情報漏えいは防げないなどの問題を提起するもの、委託先の選定として、責任範囲を明確にし、適正な・・・、総合的に・・・、実行可能な・・・という考え方だけが示され、具体性のないものであった。具体的な施策は内部では具体的に検討はしているが、それを事例として公開することができないというジレンマもあった。

調査事例1（商品説明会参加者募集等の業務委託）　・・・情セ20-SWG1-2-03-1
＞業務委託はどうすればいいの？

調査事例2（適正な業務受託契約の締結）　・・・情セ20-SWG1-2-03-2
＞責任範囲を明確にし、適正な・・・、総合的に・・・、実行可能な・・・、？？？

調査事例3（外部委託先の選定）　・・・情セ20-SWG1-2-03-3
＞ISMSやPマークを取得している会社と契約する？、再委託？

調査事例4（消費者応募キャンペーン業務の委託）　・・・情セ20-SWG1-2-03-4
＞共通認識をどのように得ればよいか？、監督内容として何を確認すればよいか？

調査事例5（イベント事務局業務の委託）　・・・情セ20-SWG1-2-03-5
＞再委託先にまで当てはめることが困難。

調査事例6（テレセールス業務の委託）　・・・情セ20-SWG1-2-03-6
＞個人情報取り扱いフロー図！

調査事例7（設備工事の請負）　・・・情セ20-SWG1-2-03-7
＞委託先とは個別に守秘義務契約等を締結しているが、・・・。P2Pソフトの個人的利用まで、・・・

調査事例8（請求書印刷等の業務委託）　・・・情セ20-SWG1-2-03-8
＞何のエビデンスをもって問題無しとするのか。？

図 2.7 収集事例と問題点

そのような中で、調査事例 6 は、個人情報の取り扱いをフロー図で示し、委託元と委託先で責任分担を明確化するものであり、「委託先の適切選定、必要な契約の締結、取扱状況の把握」の具体的な取り決めを作り出す解決の方向性を与えるものであった。

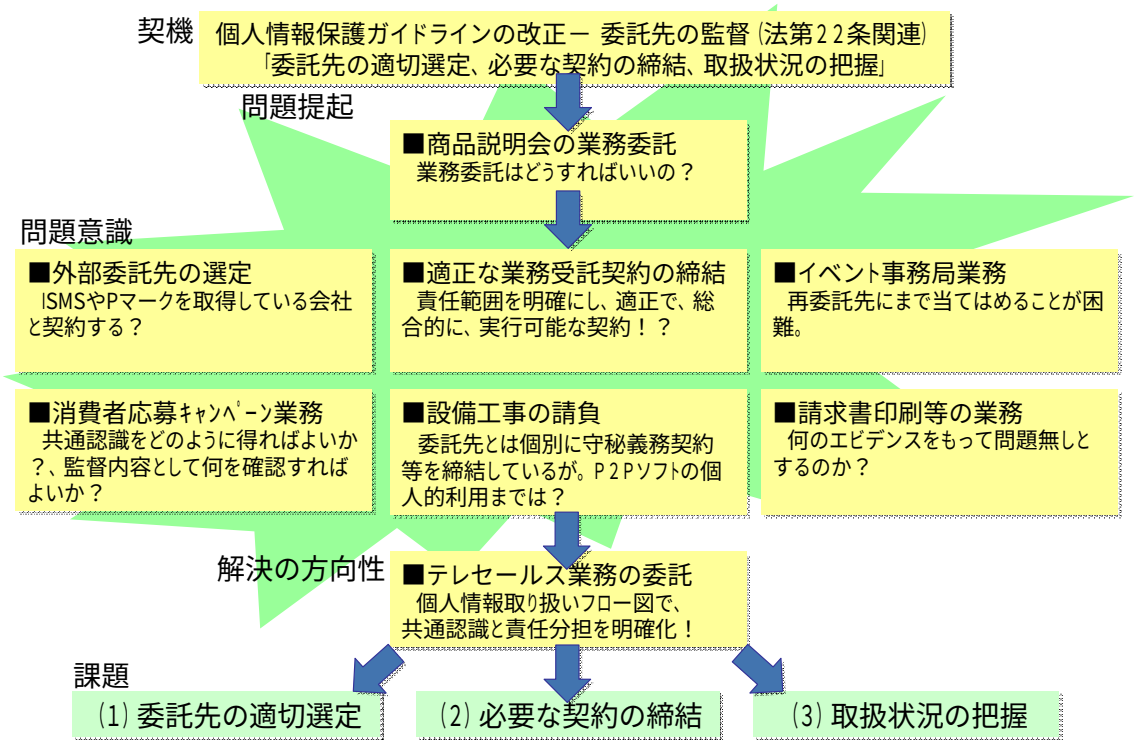


図 2.8 収集した事例の位置付け

2.4. 業務データプロセスセキュリティ評価チャートによるアプローチ

2.4.1. 本アプローチの考え方

政府等の統一基準や情報セキュリティに対する各種の評価・認定制度は企業や機能モジュールに対するあるべき姿を提案しているものである。これに対して、我々の取り組みは、業務を行う上で、実行すべき行為の取り扱いや取り決めを定めるものである。

特に、事例 6 のフローチャートは、個々に違う業務プロセス、取り扱いデータ、取扱者やそのシステム環境を明確化し、 情報セキュリティの取り決め（契約）や仕方（受け渡し、情報システム、等）を定義するのに 有効な方法を提案し、その業務を行う企業間での共通認識を得るものである。

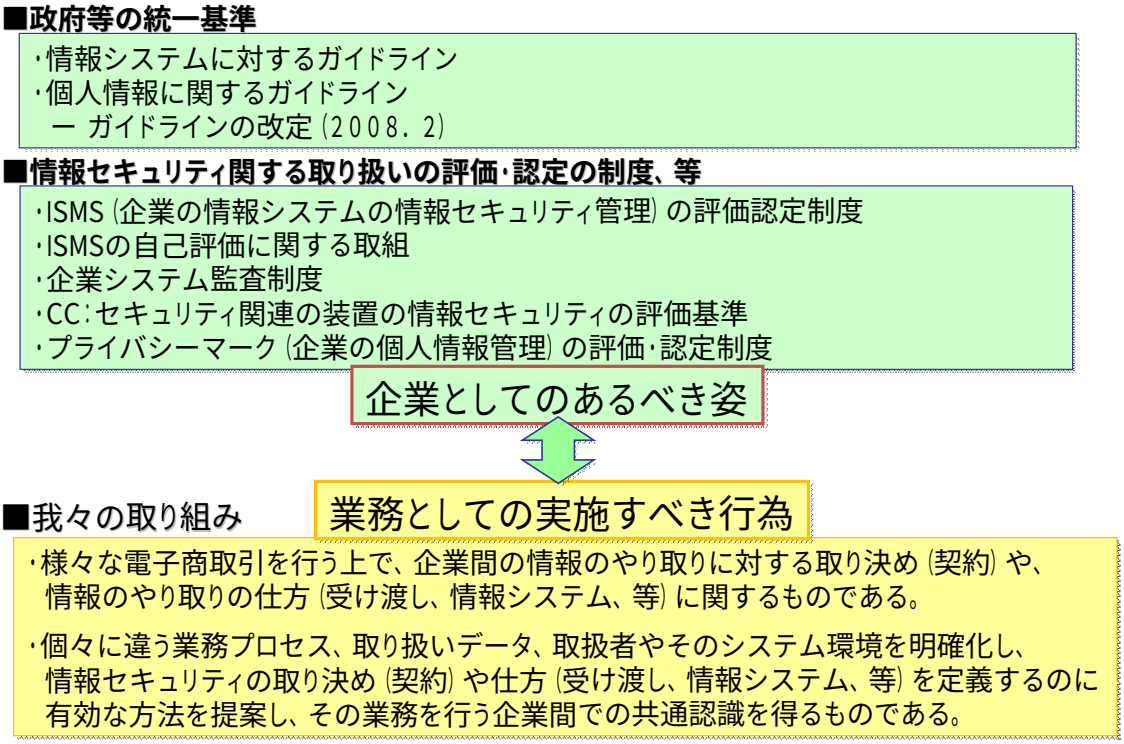


図 2.9 従来のアプローチとの違い

SWG1 では、メンバーより紹介された事例を基に、事務局が自ら経験した行事を例題として、機密保持すべき情報のフロー図を作成し、委託先の選定、契約、監督を行う際に、注意すべきポイントが明確となることを提案した。企業間での情報保護の合意形成を手順やフロー図の表記方法、記述内容に関して、紹介者に指導を受ける形で参加メンバーとともに検討を進めた。

2.4.2. 業務データプロセスセキュリティ評価チャート

（Business Data & Process Security Evaluation Chart）

業務データプロセスチャート（以下では BDP SEC と略す）の目的、特徴、記述形式の特徴を図 2.10 に示す。

（1）目的

BDP SEC は、顧客情報などの情報保護を必要とする機密データに対する処理のプロセスを明

確化する図である。 業務委託を行なう場合、①委託先の適切な選択、②委託先との契約、③取り扱い状況の把握において、 委託先と委託元で、情報保護を行なうべき責任分解点を明確とし、管理ポイントの共通認識を得る図である。

（2）特徴

図の可読性の向上の観点から、保護を必要とするデータと処理のプロセスだけを分離記述し、実施手段（計算機、ネットワーク）は記載しない。情報保護を必要とするデータに関する取り扱いは記述するが、必要としないデータは記述しない。図の縦軸は組織、横軸は時系列とし、処理の流れが変わるフェーズごとに記述する。データの発生から消滅までのフローをデータが受ける処理と処理の間で受け渡されるデータの流れを図示する。

（3）記述形式

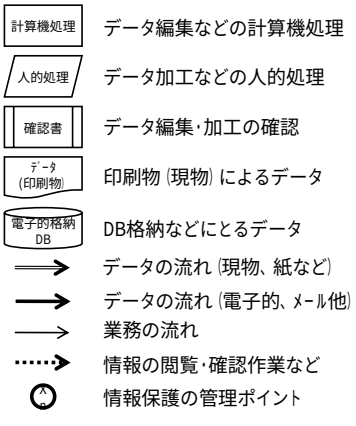
処理を示す記号（図形）は機械的に処理される処理と人間が操作する人的処理、データを示す記号はデータベースに格納されるものと、紙などの現物に印刷されるもの記号に分ける。処理を示す記号としては、処理が終了したことを確認する確認書の記号の合計 5 種類である。処理と処理の間のデータの流れは実線の矢印で示す。データの流れの矢印には流れるデータ項目を記載する。処理と処理の順序などの業務の流れは細線で示す。DB 閲覧などの確認は点線で示す。

5 種類の図形で、データの発生源から消滅の確認までのデータとプロセスの流れを記述する。その流れの中で、特に注意を要するポイントには番号を付ける。

■目的
・顧客情報などの情報保護を必要とする機密データに対する処理のプロセスを明確化する図である。
・作業委託を行なう場合、①委託先の適切な選択、②委託先との契約、③取り扱い状況の把握において、委託先と委託元で、情報保護を行なうべき管理ポイントの共通認識を得る図である。

■特徴
・処理のプロセスだけを分離記述する。実施手段（計算機、ネットワーク）は記載しない。
・保護を必要とするデータを中心として記述し、保護を必要としないデータは記述しない。

■記述形式
・図の縦軸は組織、横軸は時系列（処理の流れが変わるフェーズごとに記述分割する）。
・機密データの発生から消滅までの処理のフローを下記の記号を用いて記述する。



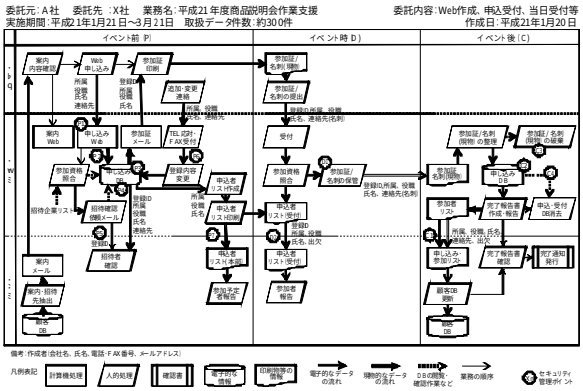


図 2.10 業務データプロセスチャート（BDP SEC）の概要

（4）作成手順

事務局が自ら経験した行事を例題として、機密保持すべき情報の BDP SEC を作成した。作成

手順を分かりやすく整理すると、大きく 5 つのステップに分かれる。作成手順を図 2.11 に示す。なお、表記方法を理解・整理しながら、説明用に BDP SEC を作成したため図 2.11 を作成するのに約 2 日かかった。記号の意味、業務分担、データの流れを理解していれば、1 日程度もあれば、十分作成可能である。

■作成手順

Step1：データの発生と結果（消去の確認）
①顧客情報などの情報保護を必要とする機密データのソース（発生源：DBなど）を記載する。
②データ処理・加工など作業を行った結果のリストや格納が必要となる中間DBを記載する。

Step2：人的作業とデータ処理プロセス
①発生源のDBなどから、中間DBや結果のリストを必要とする作業（情報の検索、加工、出力など）を抽出する。
②抽出した作業（プロセス）が人的作業か、データ処理プロセスかを決めて記載する。

Step3：委託作業と時系列
①時系列フェーズ（準備フェーズ、実行フェーズ、完了フェーズなど）に分けて、作業・プロセスを配置する。
②委託元で行なうか、作業を委託するかを決めて、作業・プロセスを配置する。

Step4：データとプロセスの流れ
①発生源のDBから、人的作業か、データ処理プロセスを経て、結果のリストなどにたどり着くように太い矢印を書く。
②データの流れで表現できていない、作業・プロセスの流れ（順序）を細い矢印で書く。

Step5：参照データと確認作業
①業務に必要となる参照データを追記する
②業務の確認作業を追記する。

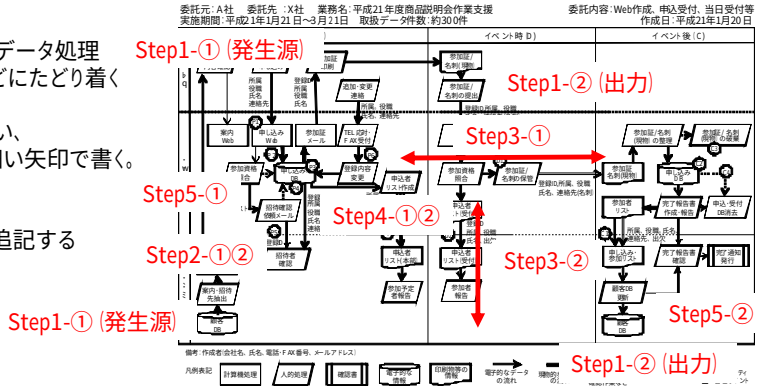


図 2.11　ＢＤＰＣの作成手順

2.4.3. 業務データプロセスセキュリティチャート作成のポイント

異なる組織間での情報保護に対する共通認識を醸成するために BDP SEC は可読性が極めて重要である。必要以上の内容を記述すると複雑となり、共通理解が得られなくなる。一方、曖昧な書き方をすると、責任分解点やリスクのあるポイントが見えなくなる。

SWG1 では、紹介事例を基に、例題（図 2.12）で、事務局自身が少し多めに記述内容を描いた BDP SEC 作成し、参加メンバーから指摘を受ける形で、作成のポイントを検討した。その結果を以下に示す。

（1）例題

A 社では毎年春に商品説明会をお得意様（約 300 名）を招き、商品説明会を実施している。A 社で商品説明会の主担当部署である宣伝部員は 3 名で、例年通り、開催案内・招待状の発送、 申込 Web の作成、申込受付、当日受付などの作業を外部委託することとした。 A 社は得意先の個人情報を有し、個人情報保護ガイドラインの改正-委託先の監督（法第 22 条関連）「委託先の適切選定、必要な契約の締結、取扱状況の把握」をどのようにすればよいかを悩んでいた。

■業務概要

－A社では毎年、春に商品説明会をお得意様（約300名）を招き、商品説明会を実施している。
－A社で商品説明会の主担当部署である宣伝部は3名で、例年通り、開催案内・招待状の発送、申込Webの作成、申込受付、当日受付などの下記の作業を外部委託することとした。
－A社は得意先の個人情報を有し、個人情報保護ガイドラインの改正-委託先の監督（法第２２条関連）「委託先の適切選定、必要な契約の締結、取扱状況の把握」をどのようにすればよいかを悩んでいた。

■作業分担

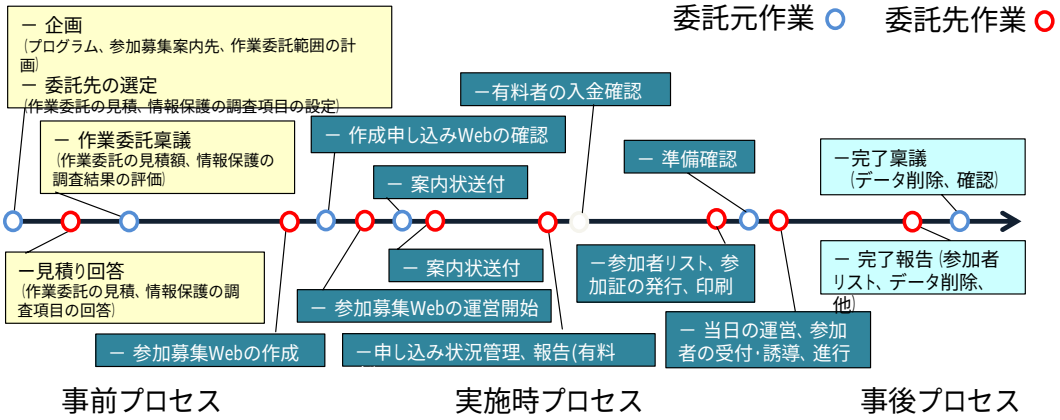


図 商品説明会の作業内容

図 2.12　例題

（2）草案の作成

前出の作成手順で示した通り、はじめに情報の発生源である顧客 DB と委託業務完了時の完了報告書を左下と右下に書き、顧客 DB から処理を記載していった。書くべきか書かざるべきかを悩んだところは記載する方向で進めた。図 2.13 は、発生源である顧客 DB から委託業務の完了報告書までつなげた図である。

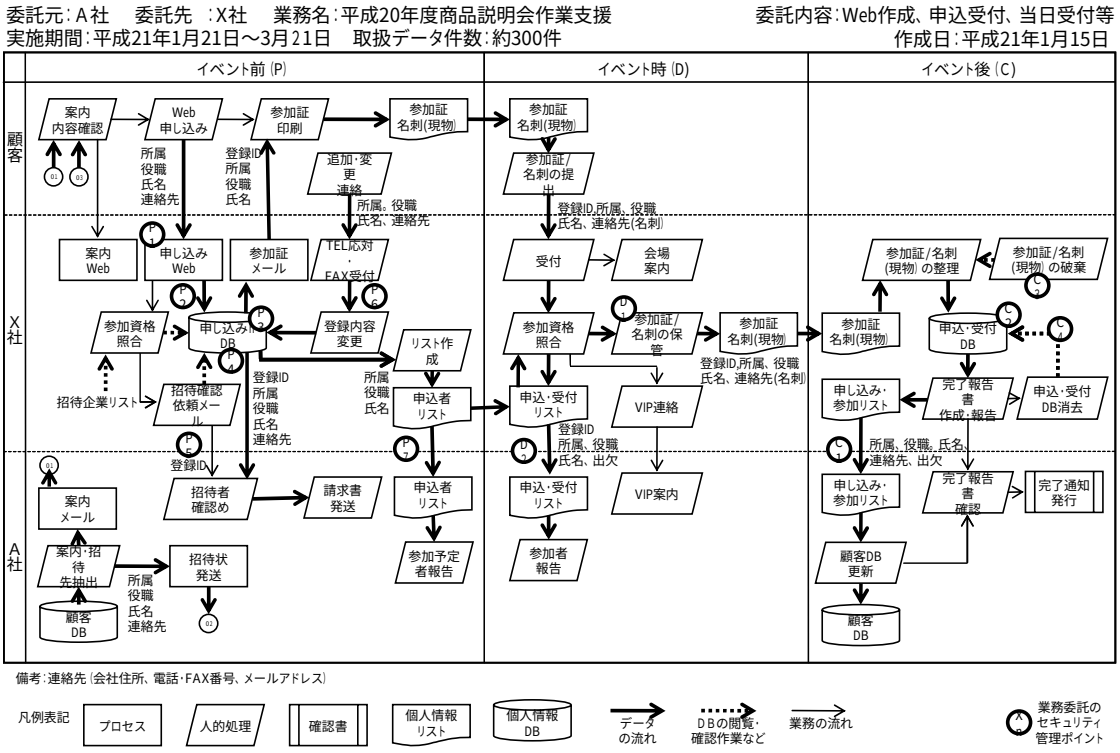


図 2.13　草案（初期作成図）

（3）レビュー

草案をベースとして、作成者が関係者に図 2.11 のフローを説明する形で、SWG1 のメンバーとともにレビューを行った。指摘を受けた内容を図に示す。指摘の内容は、可読性を向上させるためのもので、情報システムを稼働させるためにすべてのデータと処理を書くというものではなく、機密情報を管理するために、機密情報に関わるデータと処理を記述する。言い換えると管理の必要のない情報を記載すると可読性が劣化して、図をわかりづらくするばかりでなく、後で、管理工数（委託先の監督）がかかることとなる。

■指摘事項

（a）基本的に 1 つ！同じ物を複数、記述しない

（b）同じもの（DB、データ、処理）は同じ名前

（c）情報が流れる線は切らない。組織をまたがるところに、管理の観点生まれる。

（d）保護しなければならない情報がなければ、記載不要！複雑にしない

（e）矢印の向きは 左から右へ

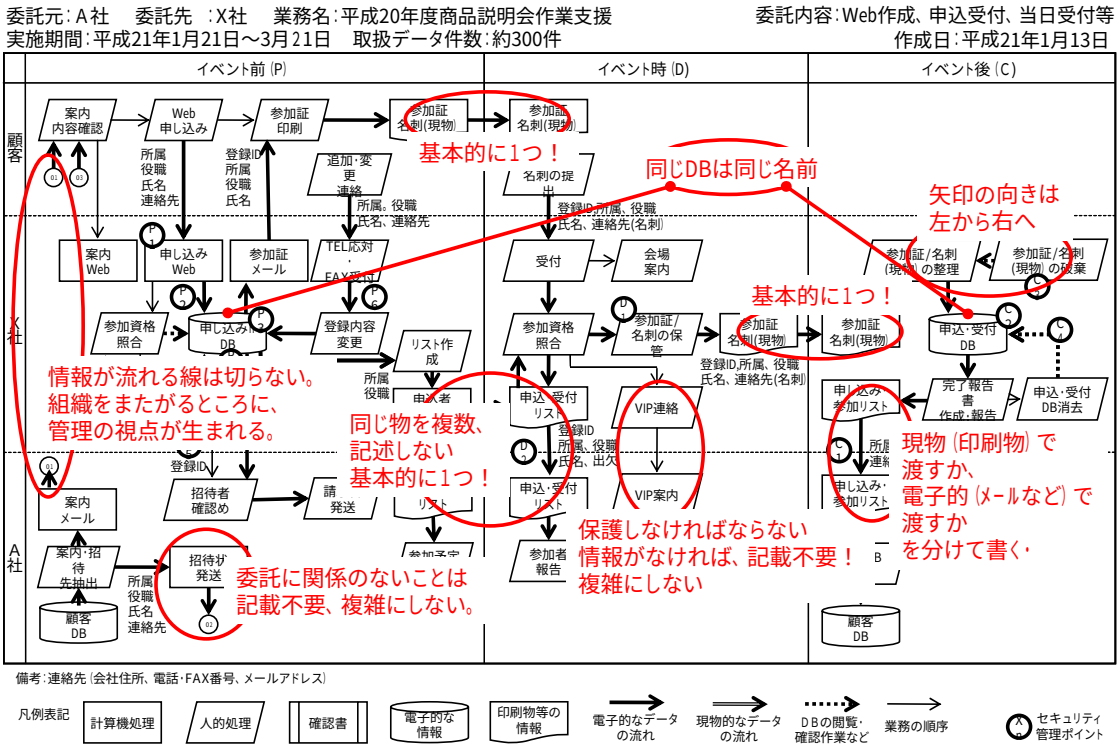


図 2.14 草案に対する指摘事項

（4）最終形

草案を関係者間で検討して、最終形にした BDP SEC を図 2.15 に示す。草案と比べて可読性が向上した。なお、可読性をよくする事だけが最終目的ではない。上記の指摘事項が絶対条件ではない。一番大切なことは、業務に係わる組織との間で、責任分解点が明確になり、企業間で情報保護が連携できるという共通認識が生まれることがもっとも重要である。レビュアーは、最終形を提出されても、それを鵜呑みにするのではなく、その図を通して、管理が必要とされる情報に抜けがないか、リスクのある部分（管理のポイント）を利用する情報システム装置の機能を含め

て、企業間で共通理解することが大切である。

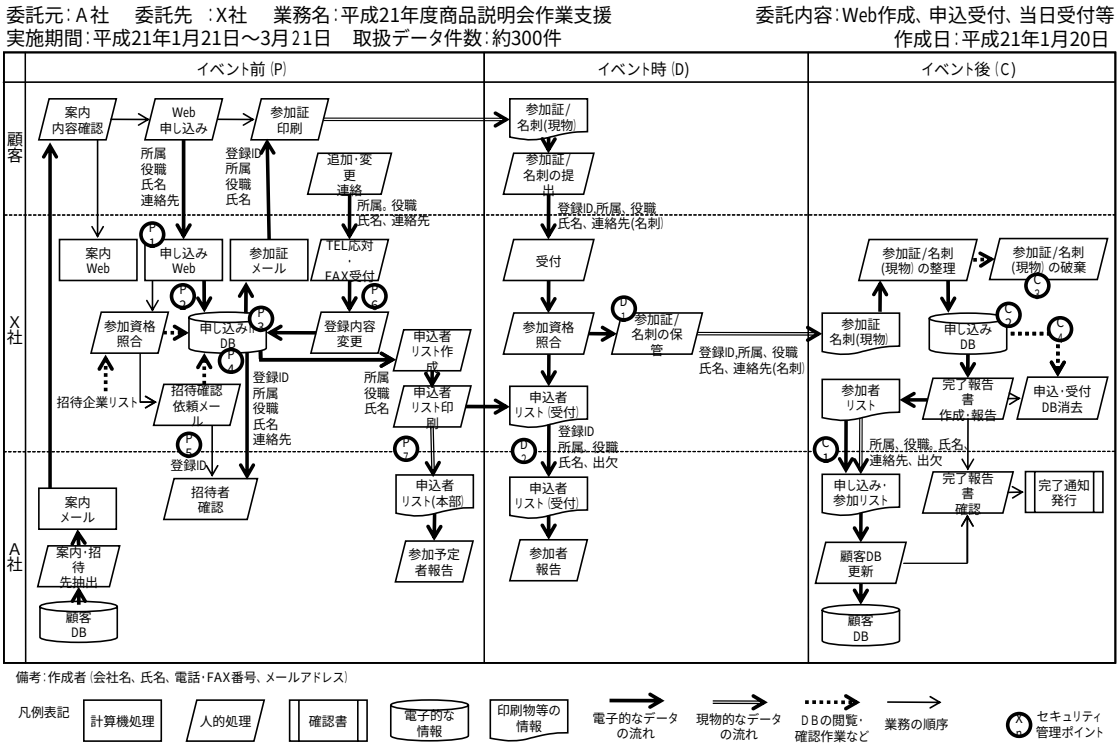


図 2.15 最終形

2.5. 本アプローチによる企業間情報連携の展開

上記では、本アプローチのコアとなる業務データプロセスセキュリティ評価チャート（BDP SEC）の特徴や作成のポイントなどを説明してきた。以下では、BDP SEC を用いた企業間情報連携を例題の委託業務で説明する。

なお、すべての委託業務、委託先に展開する必要があるというものではない。保護必要とする情報を企業間でやり取りする際に適用する。従って、まず保護する必要がある情報が何であるかということ、どのような情報主体者から入手し、どのような取り扱い制限があるかは事前に確認しておく必要がある。

委託業務に BDP SEC の利用について、前述したとおり、個人情報を取り扱う委託業務では、委託先の適切な選定、企業間での契約、委託先の監督が必要である。それぞれのステップでの適用のイメージを説明する。利用の全体の流れを図 2.16 に示す。

Step1：委託先の適切選定

委託先を決めるときは、費用見積りを取る。見積りを取る際に、BDPC を作成し、見積り条件書とともに、BDP SEC を見積り先に提示し、見積り回答を得る。見積り条件書（委託対象となる作業項目など）に添付される情報保護に関する調査書の例を図 2.17 に示す。

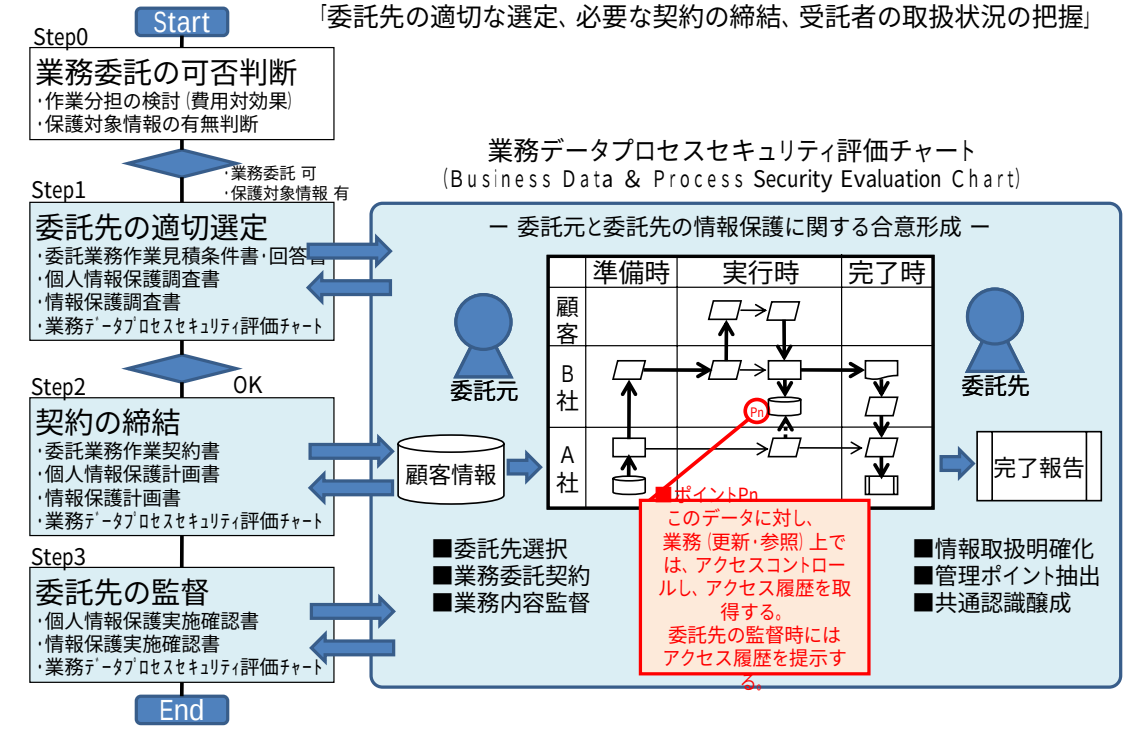


図 2.16 委託業務における BDPSEC の利用シーン

■企業の情報保護の調査票の例

情報保護に関し、御社の措置について、下記設問にご回答ください。

企業名[　　] 役職[　　] 回答者氏名[　　印]

Ⅰ. 該当項番に○をし、必要事項を記入ください。
1. プライバシーマーク取得企業（登録番号：　　）
2. ISMSの認証企業（認証範囲：　　）

Ⅱ. 現在の実施状況の該当項番に○を記入してください。
1. 対象者に個人情報保護の教育が行われ、全員が誓約している
2. 個人情報の保護方針があり、ﾎｰﾑﾍﾟｰｼﾞ等で公開している
3. 個人情報の収集に、目的の通知と収集の同意を得えている
4. 保有する個人情報が特定され、管理されている
5. 情報管理者および責任者が定められている
6. 作業場所の入退室管理が行われている
7. 情報保管庫が錠管理されている
8. 情報のアクセス制限がされている
9. 情報授受に際し、安全対策が施されている
10. 情報授受の記録がとられている
11. 情報管理に関する監査が行われている
12. 情報管理に対する相談窓口がある
13. 情報保護に関する法令及びその他の規範が特定されている
14. 外部委託の際は、機密保持契約を締結している
15. 過去において情報漏えいの事故を起こしたことがない

以上

■本委託内容の情報保護計画の調査票の例

添付の業務データプロセス図により担当業務おける情報の流れを確認し、下記の情報保護について記入してください。

企業名[　　] 部署名[　　] 氏名[　　印]

Ⅰ. イベント前（P）
P1：申し込みWebに個人情報を保護する安全措置を取るか
＞1. 正しいSSL※1、2. ID・ﾊﾟｽﾜｰﾄﾞ、3. その他（　　）、4. しない
P2：申し込みDBに外部からの不正アクセスを防止するか
＞1. 正しいWebAP※2、ﾌｧｲｱｰｳｫｰﾙ、3. その他（　　）、4. しない
P3：申し込みDBのアクセス許可管理をするか
＞1. ICカード、2. ID・パスワード、3. その他（　　）、4. しない
P4：申し込みDBのアクセス履歴をとるか
＞1. 全データ、2. ｱｸｾｽID・ﾌｧｲﾙ名、3. その他（　　）、4. しない
P5：弊社への連絡は必要最低限情報であることを考慮するか
＞1. 考慮する、2. 考慮しない
P6：TEL応対・FAX受付などでの情報、現物の管理をするか。
＞1. 台帳管理、2. アクセス者限定、3. その他（　　）、4. しない
P7：申込者リスト（現物）の受け渡しを管理するか
＞1. 台帳管理、2. アクセス者限定、3. その他（　　）、4. しない
Ⅱ. イベント時（D）
D1：会場での参加証/名刺（現物）の保管の管理をするか
＞1. 台帳管理、2. 取扱者限定、3. その他（　　）、4. しない
D2：会場での申込・受付リストの受け渡しの管理をするか
＞1. 台帳管理、2. 受渡者限定、3. その他（　　）、4. しない
Ⅲ. イベント後（C）
C1：申込・受付リストの受け渡し方法を管理するか
＞1. 暗号メール、2. 手渡し、3. その他（　　）、4. しない
C2：申込・受付DBのアクセス管理をするか
＞1. ICカード、2. ID・パスワード、3. その他（　　）、4. しない
C3：参加証/名刺（現物）破棄の確認をするか
＞1. 台帳との確認、2、アクセス者確認、3. その他（　　）、4. しない
C4：申込・受付DB消去の確認をするか
＞1. 台帳との確認、2、アクセス者確認、3. その他（　　）、4. しない

注意：
※1、※2：ECOM成果報告書：ECにおける情報セキュリティに関する活動報告書2008、ppXX1-YY1,XX2-yy2を参照のこと
御社との委託契約が成立した場合には、本調査票を御社との機密保持契約書に添付します。予めご承知置き下さい。

図 2.17 見積り作業時の調査書

左図は企業としてどのような情報保護対策をしているかという調査票である。右図は今回の案件に対して、どのようなセキュリティ対策が打てるかを調査する調査票である。左図は個人情報保護などの企業指針を管理している法務系の担当部署と作成、右図は情報システムを管理してい

るシステム部門と相談して作成することがベターである。

自社内で相談するときも、BDP SEC を利用し、どのような案件で、どのような作業分担を行い、どのようなリスクや注意点があるかを相談して、右図の調査書に条件に加えておくと、委託契約はスムーズにできる。

なお、図 2.17 の右図は今回の対象が色々な人がアクセスする可能性がある業務なので、データに対するアクセスコントロールを中心に調査票が作成されている例である。これらの条件に関しては、自社内に基準を持っていたり、PCI-DSS のように特定のデータに限定すればデータの取り扱い条件があるので、それらを参照することが臨まれる。

本アプローチでは、図 2.17 のように書けばよいということを指示しているものではない。BDP SEC を介して、それらの条件の位置付けが分かりやすくなり、共通認識が得られやすいことを提案している。契約書や調査票には企業それぞれの文化があるので、例示した契約書や調査票を規定するものではない。BDP SEC もしくはそれに順ずる図によって、責任分解点が分かりやすくなるということである。

Step2 契約の締結

図 2.18 に契約書の例と図 2.17 の右図の回答を示す。契約の締結には、業務委託誓約書、企業の情報保護調査書（回答記入済み）、本委託内容の情報保護計画の調査書、それらのリファレンスとなる BDP SEC を添付する。これにより、企業と企業での共通認識となる約束事が締結される。

■本委託内容の情報保護計画の調査票

添付の業務データプロセス図により担当業務おける情報の流れを確認し、
下記の情報保護について記入してください。
企業名[X社] 部署名[業務課] 氏名[田中一郎]

Ⅰ. イベント前（P）
P1：申し込みWebに個人情報を保護する安全措置を取るか
＞(1). 正しいSSL※1、2. ID・ﾊﾟｽﾜｰﾄﾞ、3. その他（　　）、4. しない
P2：申し込みDBに外部からの不正アクセスを防止するか
＞(1). 正しいWebAP※2、ﾌｧｲﾔｰｳｫｰﾙ、3. その他（　　）、4. しない
P3：申し込みDBのアクセス許可管理をするか
＞1. ICカード　＞(2). ID・パスワード、3. その他（　　）、4. しない
P4：申し込みDBのアクセス履歴をとるか
＞1. 全データ　＞(2). ｱｸｾｽID・ﾌｧｲﾙ名、3. その他（　　）、4. しない
P5：弊社への連絡は必要最低限情報であることを考慮するか
＞(1). 考慮する、2. 考慮しない
P6：TEL応対・FAX受付などでの情報、現物の管理をするか。
＞1. 台帳管理　＞(2). 取扱者限定、3. その他（　　）、4. しない
P7：申込者リスト（現物）の受け渡しを管理するか
＞1. 台帳管理　＞(2). 取扱者限定、3. その他（　　）、4. しない
Ⅱ. イベント時（D）
D1：会場での参加証/名刺（現物）の保管の管理をするか
＞1. 台帳管理　＞(2). 取扱者限定、3. その他（　　）、4. しない
D2：会場での申込・受付リストの受け渡しの管理をするか
＞1. 台帳管理　＞(2). 受渡者限定、3. その他（　　）、4. しない
Ⅲ. イベント後（C）
C1：申込・受付リストの受け渡し方法を管理するか
＞1. 暗号メール　＞(2). 手渡し、3. その他（　　）、4. しない
C2：申込・受付DBのアクセス管理をするか
＞1. ICカード　＞(2). ID・パスワード、3. その他（　　）、4. しない
C3：参加証/名刺(現物) 破棄の確認をするか
＞1. 台帳との確認　＞(2). アクセス者確認、3. その他（　　）、4. しない
C4：申込・受付DB消去の確認をするか
＞1. 台帳との確認　＞(2). アクセス者確認、3. その他（　　）、4. しない
以上

■情報保護計画の実施状況報告

添付の業務データプロセス図により担当業務おける情報の流れを確認し、
下記の情報保護の実施状況を記入してください。
企業名[X社] 部署名[業務課] 氏名[田中一郎]　記載日[3月15日]

Ⅰ. イベント前（P）
P1：申し込みWebに個人情報を保護する安全措置
＞1. 正しいSSL※1　＜正しいサーバー証明書※1にて実施
P2：申し込みDBに外部からの不正アクセス防止
＞1. 正しいWebAP※2　＜正しいWebAP※2にて実施
P3：申し込みDBのアクセス管理をするか
＞2. ID・パスワード　＜弊社：4名に発行、貴社：2名に発行
P4：申し込みDBのアクセス履歴
＞2. ｱｸｾｽID・ﾌｧｲﾙ名　＜不正アクセスなし
P5：弊社への連絡は必要最低限情報であることを考慮するか
＞1. 考慮する　＜基本的に登録IDのみとした。
P6：TEL応対・FAX受付などでの情報、現物の管理をするか。
＞1. 取扱者限定　＜弊社：4名に限定
P7：申込者リスト（現物）の受け渡しを管理するか
＞2. 取扱者限定　＜貴社：鈴木二郎様のみ
Ⅱ. イベント時（D）3月16日
D1：会場での参加証/名刺（現物）の保管の管理をするか
＞2. 取扱者限定　＜弊社：田中一郎、山本裕子（予定）
D2：会場での申込・受付リストの受け渡しの管理をするか
＞2. 受渡者限定　＜貴社：鈴木二郎様、佐藤浩子様（予定）
Ⅲ. イベント後（C）
C1：申込・受付リストの受け渡し方法を管理するか
＞2. 手渡し　＜完了報告時の予定
C2：申込・受付DBのアクセス管理をするか
＞2. ID・パスワード　＜田中PCにて確認完了まで保管の予定
C3：参加証/名刺(現物) 破棄の確認をするか
＞2. 取扱者確認　＜
C4：申込・受付DB消去の確認をするか
＞2. 取扱者確認　＜
Ⅳ. 懸念事項
＜不達 郵便（12、123、345）、メール（23、345）　・・・　以上

図 2.18 契約書と調査結果

Step3：委託先の監督（取扱状況の把握）

図 2.19 に委託先の監督を行なう際の取扱状況の把握に利用する調査票の例を示す。契約時点の情報保護計画の調査書に基づいて、実施状況を確認する。この際も、契約時点に、BDP SEC によりどのポイントの確認であるかを明確化しているので、調査や回答が効率的になると考えられる。

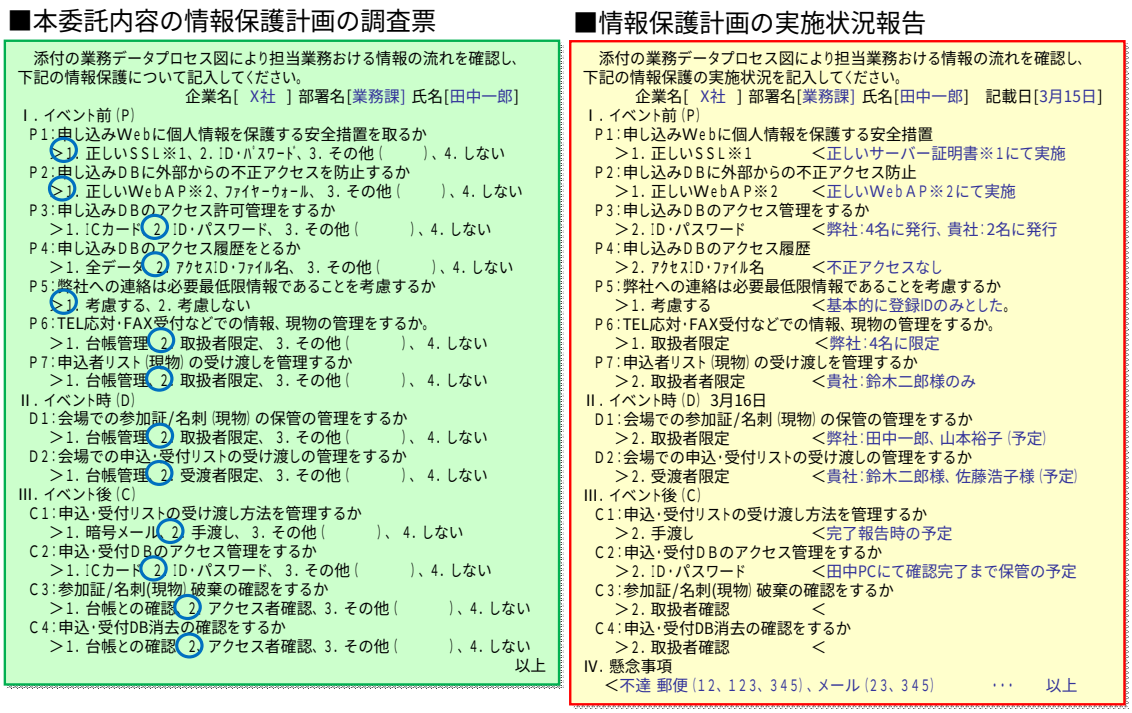


図 2.19 取扱状況の把握 (委託先の監督)

Step4:お客様 (情報主体者) へのアナウンス

上記のような委託先の適切な選定、契約の締結、委託先の監督を行なうことによって、情報主体者であるお客様に、適切な対応をしていることを宣言（図 2.20）できると考える。もし、お客様から問合せがあった場合には、BDP SEC を参照して回答すればよい。

個人情報保護や情報セキュリティにおいて、情報主体者に対して、どのように情報をどのように取り扱ってきたかということを明示的に知らせ、不安がらせないためにも、BDP SEC が必要であると考える。

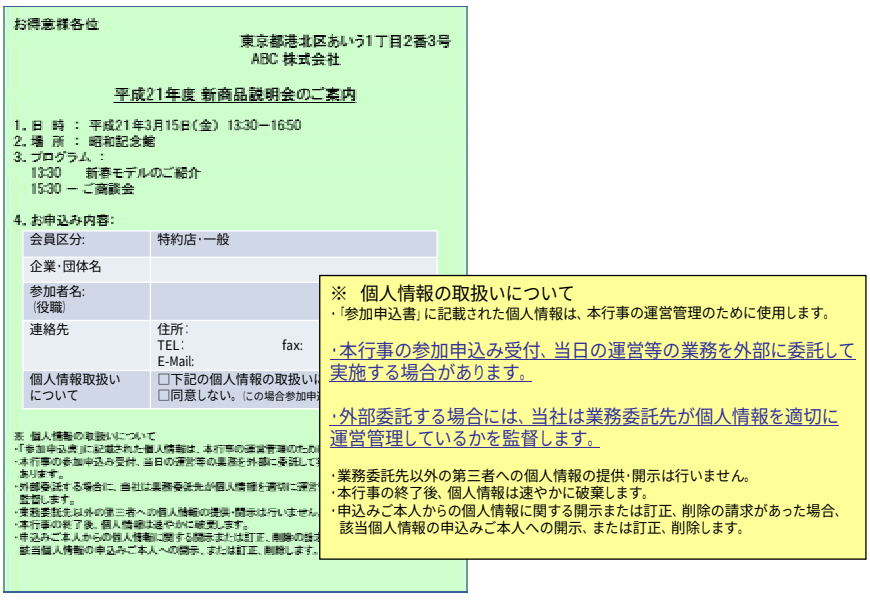


図 2.20 お客様 (情報主体者) への案内

2.6. 本アプローチのメリット･デメリット

提案してきた本アプローチのメリット・デメリットを報告する。

2.6.1. 自己評価

BDP SEC 作成者による自己評価を図 2.21 に示す。作成者自身は該当業務を 3 回経験している。情報保護の意図が委託会社に伝わらず、ひやりとしたり、心配したりした経験がある。業務の流れは頭の中にあり、危ない場面はよく理解していて、何を書くべきかは分かっている。書く内容を抽出することはさほど時間がかからなかった。どこまでの内容をどの記号を使うことが最適であるか、委託先の担当が理解できるか、というところが隘路であった。

BDP SEC を作成して、最もよかったと思うことは、頭の中にあった業務の流れやリスクが吐き出せたこと、それによって、自分自身が不安から開放されたことが大きい。委託先の担当が理解できるか？については、見積り依頼時にそれなりに説明すれば、理解が得られると感じた。

それらの説明を通じて、単にセキュリティ基準を押し付けるのではなく、委託先の事情も加味し、委託先の業務の効率も意識して、情報保護計画を立てることがこの問題（企業間情報保護連携）の 1 つの解決策であると感じた。

皆が情報を取り扱えるユビキタス社会（インターネット社会）になって、どこから情報が洩れるか、情報がどこへ行ってしまうのか、という不安感がある。この図を描くと、そのような不安感から開放され、このフローの通りに進めれば、どこか行ってしまう不安なく業務が進められるという点で、安心感が得られた。

■業務データプロセス図の作成の隘路

－Webサイト、情報処理システム、ネットワークはどのように表現するの？
－確認書とは何？
－電子媒体と現物（印刷物）は区別しなくてよいか？、リストとDBの違い
－矢印の向きは？
－複数の人に配布する参加者リストは、複数記載して良いか？

■業務データプロセス図を作成してよかったと思うこと

－データの受け渡しなど、注意すべきポイントが明確となった。
－個人情報を含むデータベースの管理ポイントを指示できるようになった。
－必要とされるセキュリティの管理レベルを指示することができるようになった。

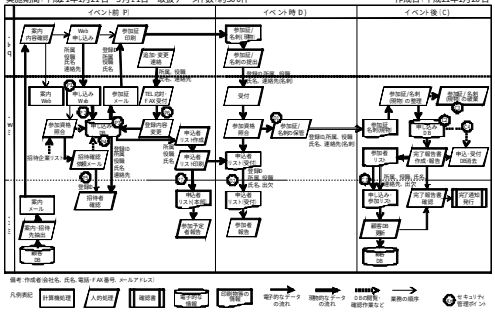


図 業務データプロセス図の例

図 2.21 自己評価結果

2.6.2. メンバーの意見

自己評価だけでは、手前味噌になるので、SWG1 メンバーにアンケートを行った。5 名のアンケート回答結果と第 4 回の SWG で出た意見を下記に報告する。アンケートの内容は、①利用について、②記載内容について、③普及について、④来年度の活動について、の 4 項目である。

回答数が少ないので、統計的な意義は持たないが、メンバーの忌憚のない個別の意見が収集できた。若干説明不足（わからない）というコメントを除き、定性的な意見を以下に纏める。なお、アンケートの資料は付録 B-1、回答は付録 B-2 に示す。

（1）利用について

■同等の図を使っているか？

回答は、同等の図を使っている、「使っていない」、「わからない」という回答に分かれた。こうした図を使って進めている企業や組織はある。きめ細かく情報セキュリティを検討している企業であったり、中小企業にセキュリティを指導している企業であったり、セキュリティの必要性を説明するために BDP SEC のような図を使っているとの回答であった。

■契約書に添付することについて

回答は「大変良い」と「どちらでもない」に分かれた。契約の内容次第で、多分、あった方が良いのだという感触である。契約に必ず添付しなければならないという規則にするということではないように思う。

■委託先の選定に利用することについて

平均すると「よい」という回答である。選定する際、守るべき資産がどのような範囲で動くのかリスクが明確になるので、遵守すべきセキュリティレベルに応じた業者を選定する必要があるので、あったほうがよい。判断材料になる。力強いコメントも寄せられた。

■ＢＤＰＣを委託先の監督に利用することについて

平均すると「よい」という回答である。よいというよりは個人情報を取り扱い管理・監督の義務が発生するので、必要である。というコメントであった。

（2）記載内容について

■ＢＤＰＣ記述内容(データの発生から消滅まで)について

回答は「大変良い」と「よい」であった。書き方の表現はいろいろありますが、データの発生から消滅までのやり取りを明確化することは必要である、組織的な情報管理の姿として 1 つの方向だと思います、というコメントであった。

■ＢＤＰＣの記述内容（情報セキュリティに対する装置、システム、機能を記述しない）について

回答は「大変良い」から「よくない」に分かれた。システムの機能に関しては BDP SEC とは別で整理したほうがよい、あくまでも BDP SEC はデータのプロセスのみ明記する、他のドキュメントで補完できるならそれでも良いのでしょう、面倒かも、などの意見分かれた。第 4

回の SWG で検討した結果では、システム機能（暗号方式など）を記述すると、色々と異なるレベルや区別すべき記号が増え、複雑になるので、やめるべきという意見であった。

■ＢＤＰＣの作成で使用する記号（表記方式）について

回答は「大変良い」と「どちらでもない」という意見であった。理由等のコメントがなかったが、第 4 回の SWG で検討した結果では、それですべてかけるのか、どこまでかけるのかということがみえてこないため、どちらでもないという回答になっている。事例によって、検証していくことが必要ではないかと感じた。

■ＢＤＰＣの作成で参考となる例（基本例のみ）について

アンケートの回答は「どちらでもない」にまとまった。しかしながら、再委託を許可した場合複雑化すぎる、このフォーマットに決めてしまうと、再委託、複数者の業者へ委託する場合書けない、1 枚に複数業者を書く場合、どこまでオープンにするかなどよく考えないといけない、適当な雛形が無いと、新しい取り組みをしたがらないのでは？というコメントがあった。回答とは裏腹に、いくつかのパターンでの事例がないと適用する上では、疑問が生じ、効率の良い実施にはならないと感じた。

（3）普及について

■自社内や委託業務でＢＤＰＣによる共通理解の推進について

回答に「実施しない」はなかった。コメントとしては、同じフォーマット、ルールではないが、社内の基準に従い、既に行っている、まともな組織を考えるなら、検討対象の 1 つだ、であった。すでに実施している企業は、既存のやり方を踏襲したいというのが、実情である。

■ＢＤＰＣの表記方式の標準化について

アンケートの回答は「よくない」であった。コメントとしては、まずは報告程度を目標とし、コンセンサスの範囲・度合いに応じて標準化のレベルをグレードアップする方法も考えられる、推奨にとどめ詳細は各社様式を定めればよい、今段階でわざわざ標準化レベルまでする必要はないのではないか？、QMS という基準があり、その図を活用すれば標準化になるのではない？、とりあえず自由にやらせてみては、という意見である。

第 4 回の SWG で、色々なコメントが出たので、検討をした結果を次節で報告する。

■業務データプロセスセキュリティ評価チャートという名前について

回答は「どちらでもない」という意見である。業務データのうち保護対象のみ記載するので、単に業務データとしない。機密情報及び個人情報のみに実施させるのであれば、BDPC ではないような気がする、とのコメントであった。

第 4 回の SWG では、本アプローチの新規性についても議論した。従来からシステム・ソフト開発分野、品質管理分野 QMS、プロジェクト管理分野 PMBOK など、類似した図表は存在する。

情報セキュリティ分野という意味を入れて、和名：業務データプロセスセキュリティチャー

ト、英名：Business Data Process Security Evaluation Chart と ECOM では呼ぶことにした。

（4）企業間情報保護連携（SWG1）の来年度の活動について

■ＢＤＰＣによる共通理解の普及について

回答は「よい」という回答であった。 共通理解はよいのだが、普及させるには「普及版」が必要ではないかと思う。今年度のフローで中小企業に普及させるには予算・人員でかなり無理があると思う。導入に必要な条件の検討と表示が必要、他のソリューションとの比較表の添付もいる、普及することについてはよいと思う。

■企業間情報保護連携で来年度実施すべきテーマについて

意見としては、費用の少ない普及版の検討、具体的な情報のモデル（種類：CAD、個人情報、会計情報）を使った事例の作成が挙げられた。

■安全･安心ＥＣ環境整備として来年度実施すべきテーマについて

意見としては、最近多くの企業や団体で検討が始まっている「秘密分散技術」を利用したセキュリティ。「電子割符」を用いた安全・安心技術に関するテーマ、もっと実社会との連携を密接に感じられる情報システムとのインターフェース・認証・セキュリティシステムの必要性の調査、が挙げられた。

2.6.3. 本アプローチの有用性と新規性

本アプローチは、参加メンバーの事例を基に、参加メンバーから現場の声ややり方のコメントをベースとしている。個人情報保護法に対応して、少なくとも契約書に BDP SEC のような図の添付を義務付けているのは紹介者の企業だけであった。

個人情報保護や情報セキュリティをきめ細かく検討している企業の現場でのメモ書きまで含めれば、様々な形の図を用いて、情報がどのように流れ、どのような扱いを受けているかは検討されている。

きわめて複雑な問題に対して、図形を用いて標準化した記述形式を使うことの意義は、複雑な事象をわかりやすくしたり、分析、共同作業ができるようにしたりするところにある。データや処理の流れを図形で表現した代表例としては、システム・ソフト開発分野の PAD（Problem Analysis Diagram）、品質管理分野の QMS(Quality Management System)のツール、プロジェクト管理分野の PMBOK のツールなどがある。

有識者よりご指導いただいた情報伝達の電子的伝達と現物手渡しの違いも入れて、本アプローチ（データプロセスセキュリティ評価）をモデル化すると下記のとおりである。

なお、最終的なワークシートを付録 C に示す。

業務データプロセスセキュリティ評価モデル

■分野：情報セキュリティの評価

■目的：情報セキュリティ（情報保護）の可読性向上と要件（注意点）抽出
　　責任分解点の明示化

■特徴：業務データプロセスと情報セキュリティマネージメントシステムの記述分離
■記述内容：機密情報の発生から消滅までの処理とデータの流れ
■記述形式：
－チャート（A4 もしくは A3）
・横軸　　処理フェーズ　　（準備、実行、完了など）
・縦軸　　情報主体（機密情報源)、情報取扱者甲、乙
－タスク：図形 5 種類、矢印 4 種

・業務処理（計算機処理、人的処理　）	図形 2 種
・確認処理（確認書など）	図形 1 種
・記憶媒体（電子的格納、現物(紙等)）	図形 2 種
・情報伝達（電子的伝達、現物手渡し）	矢印 2 種
・情報参照	矢印 1 種
・順序制御	矢印 1 種

本モデルは業務として行う情報の処理・格納・参照を情報セキュリティとしての特性（リスク発生の特性）の違いを表現したものである。これまでの参加メンバーや有識者の意見を聞く限りでは、企業間の情報保護連携において、上記のモデルが特性として組み込まれており、BDP SEC の有用性があると考えられる。

なお、本 SWG は現場の声や専門家の意見を集めて、企業間での情報保護の連携の手段として、有効性の議論を中心に検討してきたので、本アプローチの新規性について議論をしてこなかった。

先進技術として誰も使っていないというような技術の進歩性はないが、情報管理技術（マネージメントテクノロジー）として、どの範囲で、どのようなことを誰に対して明示化し、責任分解点を共有することで、どのような効果を生み出すのかという点でより良いものがないかの調査することも必要である。

2.6.4. 業務データプロセスセキュリティ評価チャートの標準化と利用シーン

アンケート結果と第 4 回の SWG で検討した結果では、皆、標準化という名前で、強制されるのを嫌がっている。情報システムの標準化のようにこの仕様に準拠していなければ、相互運用性がない、システムが動かないというわけではないので、標準化のコストを除けば、否定する必要はない。

特に、今回の対象（委託業務の個人情報保護）では、1 対 1 の契約行為であるので、双方が合意すれば、標準仕様で記述する必要はない。いくつかの現場では様々な書き方が存在し、それを 1 つに記法に強制する必要性はない。全体的な意見は、必要に応じて標準化されたものを利用すべきという意見である。

標準化した記述形式を使うことの意義は、複雑な事象において、異なる専門家による意見の交換、ノウハウの共有と蓄積、相互理解の効率化、であると考える。そのような観点も含め、第 4 回の SWG 等で出た利用シーンの例としては以下のものが挙げられる。

（1）BDP SEC のような図を導入していない企業・団体での利用
・企業間の業務委託だけでなく

・企業の中の組織など、責任の所在がわかれるような場合
・機密情報管理が組織と組織の間で押し付けあいになるような場合
・専門分野が違う複数の組織の場合など
想定効果：異なる専門家による意見の交換、ノウハウの共有と蓄積、相互理解の効率化

（2）様々な企業や企業間での情報保護のあり方を聞かなければならないシーン
・個人情報漏洩を起こした様々な企業の主務大臣への報告
（特に、最終的な報告としての原因と改善策）
・企業や企業間での情報保護のあり方を管理する必要がある公共的な機関
想定効果：異なる専門家による意見の交換、ノウハウの共有と蓄積、相互理解の効率化

（3）情報保護をしている（セキュリティある）サービスであることを説明するシーン
・消費者等の情報弱者への説明において、公的な表現をもって説明する場合
・サービス提供者が複数の提供先と提携する場合。
想定効果：異なる専門家による意見の交換、ノウハウの共有と蓄積、相互理解の効率化

（4）越境（異なる国）での情報共有ルールを明確する必要があるシーン
・機密情報（例えば、設計図）などを用いた国際間で業務を行う場合
（言葉が異なり、特に図表による周知徹底が必要な場合）
想定効果：異なる専門家による意見の交換、ノウハウの共有と蓄積、相互理解の効率化

2.7. おわりに

企業間情報保護連携ガイド作成事業の初年度として行ってきた活動の成果と今後の課題をまとめる。

2.7.1. 活動成果

本事業の初年度の活動として、本活動対象のスコープを設定するとともに、個人情報の保護に関する法律についての経済産業分野を対象とするガイドラインの改正における「委託先の適切選定、必要な契約の締結、取扱状況の把握」を例として、参加メンバーが収集した事例（委託業務契約や問題点）から課題を明確化した。

各企業で行っている企業間情報保護連携のやり方を参考として、解決の方向性を導出した。本解決アプローチは業務データプロセスセキュリティ評価チャート（BDP SEC）より異なる組織の関係者間で情報保護に関する合意形成を行うものである。メンバーより紹介された事例と ECOM 行事を基に BDP SEC の例を事務局で作成した。作成した例を参加メンバーや有識者とともに有効性を評価した。

有効性があるとのメンバーの声により有識者からの改善点を加味し、企業間情報保護連携のためのデータプロセスセキュリティをモデル化し、利用イメージを検討した。本方式は複雑な情報

セキュリティ問題の可読性を向上させ、案件ごとに実行性のある情報保護のポイントを関係者との合議により導出するものである。以下に活動成果をまとめる。

（1）企業間情報保護連携の検討対象

企業間情報保護連携活動の初年度として、検討を行うスコープを設定し、初年度に取り扱う対象を決定した。

■対象情報のスコープ　＜初年度の検討対象

・情報の種類（人、物、金）　＜個人情報

・秘匿性（厳秘、（秘）、関係者外秘、開示、公開）　＜関係者

・取り扱い（期間、アクセス回数、アクセス人数）　＜有期、多アクセス、数名

■情報共有の形態

・関係者数（1 対 1、1 対 N、N 対 M、N 対 N）　＜1 対 1（企業間）

・関係（対等、上下、委託）　＜委託関係

（2）企業間情報保護連携の課題

企業間での業務委託での個人情報保護を具体例として、参加メンバーとともに現場の声から、情報保護の課題を明確化した。

■共通した情報保護基準作成の困難性

委託業務において、委託する範囲、取り扱う情報が千差万別であり、共通した基準やセキュリティ対策や評価も千差万別である。共通した情報保護基準を作ることは困難である。

■委託契約事項（情報保護要件）の具体性の欠如

メンバーが集めた委託契約事項や問題事例では、「総合的に、合理的に、適切に」といった抽象的な表現により契約が交わされるもので、具体的な情報保護基準を定めたものがなかった。契約を交わしていても、具体的な情報保護対策を要求するものではなく、情報漏洩などの事案につながっていた。

■業務に携わる関係者間での共通理解・共通認識の重要性

紹介事例により、情報の発生から消滅までの個人情報と業務プロセスのフロー図を用い、「業務に携わる関係者間での複雑で不確実なリスクの共通理解」と「そのリスクに対する情報保護対策の共通認識」の重要性を参加メンバーは共有した。

（3）業務データプロセスセキュリティチャート（BDPSEC）と解決の利用例

紹介事例や有識者の指摘により、BDP SEC の作成目的、記述形式、作成手順、作成上のポイントを作成した。個人情報に対する委託業務の「委託先の適切な選択、適切な契約の締結、委託先の監督」に対する具体的な利用例を作成し、企業間情報保護連携として必要とされるアプローチであることの共通認識を参加メンバー間で醸成した。

（4）データプロセスセキュリティ評価モデルの作成

有識者の指摘により、情報伝達の電子的伝達、現物手渡しの区別を追加し、BDPSC を情報セキュリティの特性に分けた記述形式に改良し、データプロセスセキュリティ評価モデルを作成し

た。

（5）標準化した場合の利用シーンと想定効果

BDPSC の利用シーンを検討し、それらの想定効果を作成した。

■BDPSC のような考え方を導入していない企業・団体での利用

■様々な企業や企業間での情報保護のあり方を聞かなければならないシーン

■情報保護をしているサービスであることを説明するシーン

■越境（異なる国）での情報共有ルールを明確する必要があるシーン

なお、本評価モデルを ECOM スタイルとすることを参加メンバーで合意した。

2.7.2. 今後の課題

企業間情報保護連携の初年度活動としては、参加メンバーの協力と事務局の努力により、課題の認識からデータプロセスセキュリティモデルまで作成することができた。

今回のアプローチは、委託業務を例として、情報保護対策のあるべき姿を追いかけてきた。基本的な考え方は、複雑・不確実なセキュリティ問題（どこに問題点が潜んでいるか分からない問題）に対して、専門の異なる関係者がそのリスクや対策を共通認識と共通理解を得るための図である。今後の課題を以下に示す。

（1）本アプローチの普及と標準化

事例の紹介企業では、すでに数多くの案件で、委託契約書に義務付けている。ある意味、個社で普及が始まっている。この取り組みを支援する意味でも、まだ、図を使って具体的なセキュリティ対策のコンセンサスを得ていない企業もしくは企業間に対して、この取り組みを普及させていくことが重要である。普及の方向性としては下記のとおりある。

■ECOM 関係者への普及

今年度は、ECOM 会員企業・団体への普及として、ECOM セミナーを開催し、紹介企業を講師に招き、企業としての取り組みを紹介し、好評であった。今後、ECOM 会員へ広げていく意味でも、図を使って具体的なセキュリティ対策のコンセンサスを得ているかの ECOM 会員アンケートを広く実施することが必要である。

■トラブルの検証、改善提案への普及

関係者のコンセンサスが得られていなかったり、情報が飛散したり、システム・ソフトの対策が不十分だったりすると、情報はどこかから漏れ出す。言い換えるとトラブルを起こす。このアプローチの評価は保護のリスクや対策に対し図を使って、異なる専門家の参画してあぶり出せるかである。トラブルの検証、改善提案に使うことによって、ノウハウが共有できることになる。

■情報処理を正しく発展させたい国や企業への普及

一定の範囲で共通化が実施できれば、図は言葉の異なる人たちとの相互理解につながる。本

アプローチは情報の取り扱いを明示的にして、情報の漏えいや飛散を防ごうとするものである。情報の漏えいや飛散を防ぎたくない国や企業を除き、情報処理を正しく発展させたい国や企業への普及を推進していくことが、世界全体の正しい情報処理につながる。

（2）本アプローチの拡張

企業間情報保護連携の最終的な目標は図を書くことではない。図を書くことによって、関係者のコンセンサスを得たり、情報が飛散しないようにしたり、システム・ソフトの対策が取ることである。

本アプローチでは業務プロセスを情報保護の視点で図式化している。システム・ソフトに関するモデル化は、専門性が強くなりすぎ、異なる専門家との共通理解の妨げになるので、あえてはずしてきた。しかしながら、情報システムのセキュリティ対策も重要な視点である。これに対して、現在の図の中に取り込んでいくと、異なる専門家との共通理解の妨げになるので、本図で示される業務処理などがどのような企業や企業間の情報システムのセキュリティ装置の上で行われるかをモデル化することが次の課題である。

企業間情報保護連携 SWG（SWG1）メンバーリスト

（敬称略）

参加区分	氏名	会社名
会員メンバー	青山　彰	花王株式会社
	保倉　豊	グローバルフレンドシップ株式会社
	川城　三治	グローバルフレンドシップ株式会社
	鈴木　靖	大日本印刷株式会社
	中田　幸枝	パナソニック株式会社
	高瀬　秀一	電気事業連合会
	白川　昭久	（株）シーピーデザインコンサルティング
	保坂　弘史	株式会社リコー
	吉竹　弘幸	みずほ情報総研株式会社
	行木　直之	マイクロソフト株式会社
有識者	辻　　秀一	東海大学
	荒川　一彦	近畿大学
	成瀬　一明	株式会社　東芝
	岩田　修	オフィス　イワタ
	高橋　和博	株式会社テプコシステムズ
	垣内　伯之	日本情報処理開発協会
オブザーバー	清水　友晴	経済産業省 情報セキュリティ政策室
	和田　浩明	経済産業省 情報セキュリティ政策室
WG 主査	再起　和夫	パナソニック株式会社
事務局	合原　英次郎	次世代電子商取引推進協議会
SWG リーダ	川嶋　一宏	次世代電子商取引推進協議会

参考文献･資料

[2.1] ECOM：EC における情報セキュリティに関する活動報告書 2007(平成 20 年 3 月)
http://www.ecom.jp/results/results19.html
[2.2] PCI Security Standards Council：Payment Card Industry Data Security Standard (PCI DSS)
https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml
[2.3] VISA/JCB：PCI データセキュリティスタンダード, バージョン 1.0（2004 年 12 月）
[2.4] 北岡弘章：アウトソーシングとセキュリティ対応（1）情報の性質を踏まえた委託先管理や契約が必要, 知っておきたい IT 法律入門, ITPRO（2008/01/18）
http://www.itproexpo.jp/article/COLUMN/20080116/291207/
[2.5] 北岡弘章：アウトソーシングとセキュリティ対応（2）ガイドライン改正内容から委託先管理の問題点を検討する, 知っておきたい IT 法律入門, ITPRO（2008/02/05）
http://www.itproexpo.jp/article/COLUMN/20080129/292294/
[2.6] 北岡弘章：アウトソーシングとセキュリティ対応（3）リスク管理ツールとしての契約書作成の留意点（2008/02/15）
http://www.itproexpo.jp/article/COLUMN/20080213/293708/
[2.7] 経済産業省：個人情報の保護に関する法律についての経済産業分野を対象とするガイドラインの改正－委託先の監督（法第 22 条関連）
http://www.meti.go.jp/policy/it_policy/privacy/080229kaisei-guideline.pdf

2-3. 企業間情報保護連携ガイド策定･利用促進

⑴ 概 要

情報セキュリティ対策は、大企業を中心に各種の法律・ガイドラインや各種の関連団体の活動によって整備が進んできたが、中小、零細な企業では十分な対応や対策ができておらず、個人情報（顧客情報）だけでなく、営業情報（設計図面など）が流出するというケースも起きている。

個人情報の保護に関する法律についての経済産業分野を対象とするガイドラインの改正が本年 2 月に行われた。その主な内容は、委託先に対する必要かつ適切な監督内容の明確化であり、「委託先を適切に選定すること、受託者との間で必要な契約を締結すること、受託者における委託された個人データの取扱状況を把握すること」、があげられている。

先進的な情報保護（情報セキュリティ対策）を行う企業（委託者）では、様々な情報保護の運用・管理の調査項目を多数有しており、監督内容の明確化が厳密になればなるほど、異なる業界の業務を受託する企業、特に中小、零細な企業は、調査項目に回答することさえも困難な状況に追い込まれる。

こうした状況を踏まえ、電子商取引分野において、委託者が受託者に対する調査項目や要求する契約項目の意味に対する共通理解を醸成し、情報保護における委託者と受託者での役割分担を明確化し、企業間が連携した情報保護を行うことによって、安全・安心 EC 環境の整備を推進し、中小企業、零細企業を含む産業界の情報セキュリティの底上げに資する。

⑵ 活動内容

①委託先に対する個人情報保護の調査項目のヒアリングと整理

異なる業界で先進的な情報保護を行う企業が委託先へ最低限行う調査項目を集め、その調査項目の意味と受託者が回答を行う上での判断基準を整理する。

②委託先に対する情報保護の調査項目のガイドの作成

その調査項目の意味と回答基準の整理で得られた知見をもとに、共通した安全・安心 EC 環境の整備として公開できるものをガイドとしてまとめる。

③啓発資料としてパンフレットの作成

電子商取引を利用する関連企業、中小企業、零細企業への啓発資料としてパンフレットを作成する。

(3)活動計画

①実施体制

先進的な情報保護を行う ECOM 会員、中小企業、零細企業でも実現できる仕掛け、仕組みを検討・提供できる ECOM ベンダー会員によりワーキンググループを組織し活動する。

②実施計画（2 年間を予定）

平成 20 年度：委託先に対する個人情報保護を中心とした調査項目のヒアリングと整理

平成 21 年度：委託先に対する個人情報保護を中心としたガイドパンフレットの作成

付録 B-1 メンバーへのアンケート 資料

資料:情セ20-SWG1-4-3

ECにおける企業間情報保護連携
業務データプロセスチャート
アンケート

- 情報セキュリティ対策の共通認識に向けて -

次世代電子商取引推進協議会(ECOM)
情報セキュリティWG SWG1事務局
2008年 12月

ECOM 情報セキュリティWG 企業間情報保護連携SWG1ではECにおける企業間での情報保護の共通認識に向けて、委託業務における企業間で契約書に添付する業務データプロセスのチャートの検討を進めています。

図の作成や利用において、長所、短所、問題点、改善点などを纏めていきたく、アンケート(P13－P16)にお答えいただけると幸いです。

ご協力のほどお願い申し上げます。

ECOM
情報セキュリティWG
企業間情報保護連携SWG
事務局 川嶋

1. 業務データプロセスチャートについて

■目的

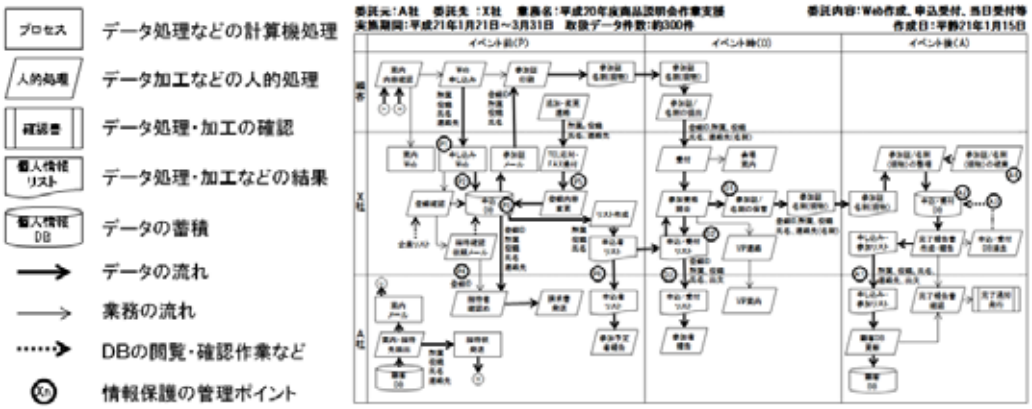
・顧客情報などの情報保護を必要とする機密データに対する処理のプロセスを明確化する図である。
・作業委託を行なう場合、①委託先の適切な選択、②委託先との契約、③取り扱い状況の把握において、委託先と委託元で、情報保護を行なうべき管理ポイントの共通認識を得る図である。

■特徴

・処理のプロセスだけを分離記述する。実施手段(計算機、ネットワーク)は記載しない。
・情報保護を必要とするデータは記述し、必要としないデータは記述しない。

■記述形式

・図の縦軸は組織、横軸は時系列(処理の流れが変わるフェーズごとに記述分割する)。
・機密データの発生から消滅までの処理のフローを下記の記号を用いて記述する。



2. 業務データプロセスチャートの作成手順

■作成手順

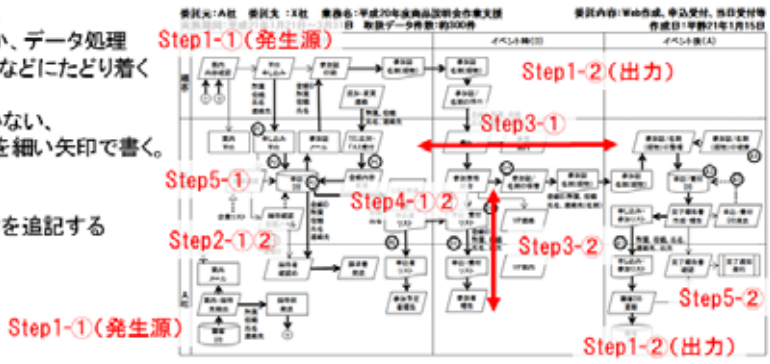
Step1:データの発生と結果
①顧客情報などの情報保護を必要とする機密データのソース(発生源:DBなど)を記載する。
②データ処理・加工など作業を行った結果のリストや格納が必要となる中間DBを記載する。

Step2:人的作業とデータ処理プロセス
①発生源のDBなどから、中間DBや結果のリストを必要とする作業(情報の検索、加工、出力など)を抽出する。
②抽出した作業(プロセス)が人的作業か、データ処理プロセスかを決めて記載する。

Step3:委託作業と時系列
①時系列フェーズ(準備フェーズ、実行フェーズ、完了フェーズなど)に分けて、作業・プロセスを配置する。
②委託元で行なうか、作業を委託するかを決めて、作業・プロセスを配置する。

Step4:データとプロセスの流れ
①発生源のDBから、人的作業か、データ処理プロセスを経て、結果のリストなどにたどり着くように太い矢印を書く。
②データの流れで表現できていない、作業・プロセスの流れ(順序)を細い矢印で書く。

Step5:参照データと確認作業
①業務に必要となる参照データを追記する
②業務の確認作業を追記する。



商品説明会の委託業務　　例題

■業務概要

－A社では毎年、春に商品説明会をお得意様（約300名）を招き、商品説明会を実施している。
－A社で商品説明会の主担当部署である宣伝部は3名で、例年通り、開催案内・招待状の発送、申込Webの作成、申込受付、当日受付などの下記の作業を外部委託することとした。
－A社は得意先の個人情報を有し、個人情報保護ガイドラインの改正-委託先の監督（法第22条関連）「委託先の適切選定、必要な契約の締結、取扱状況の把握」をどのようにすればよいかを悩んでいた。

■作業分担

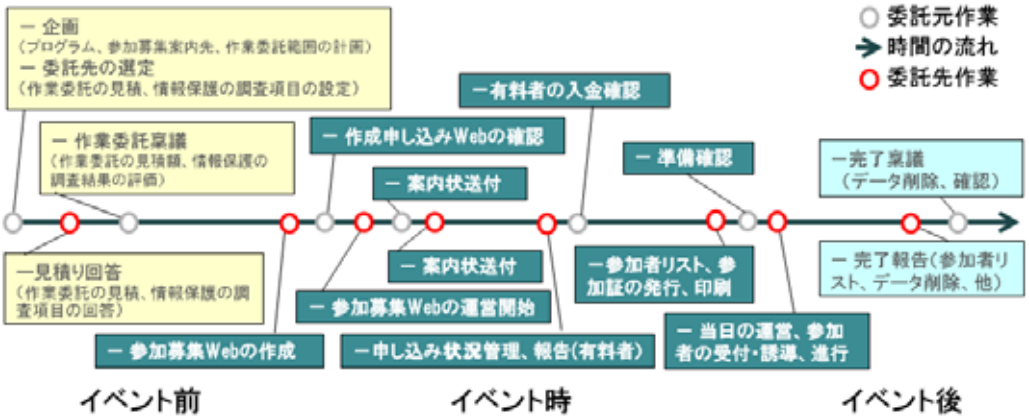
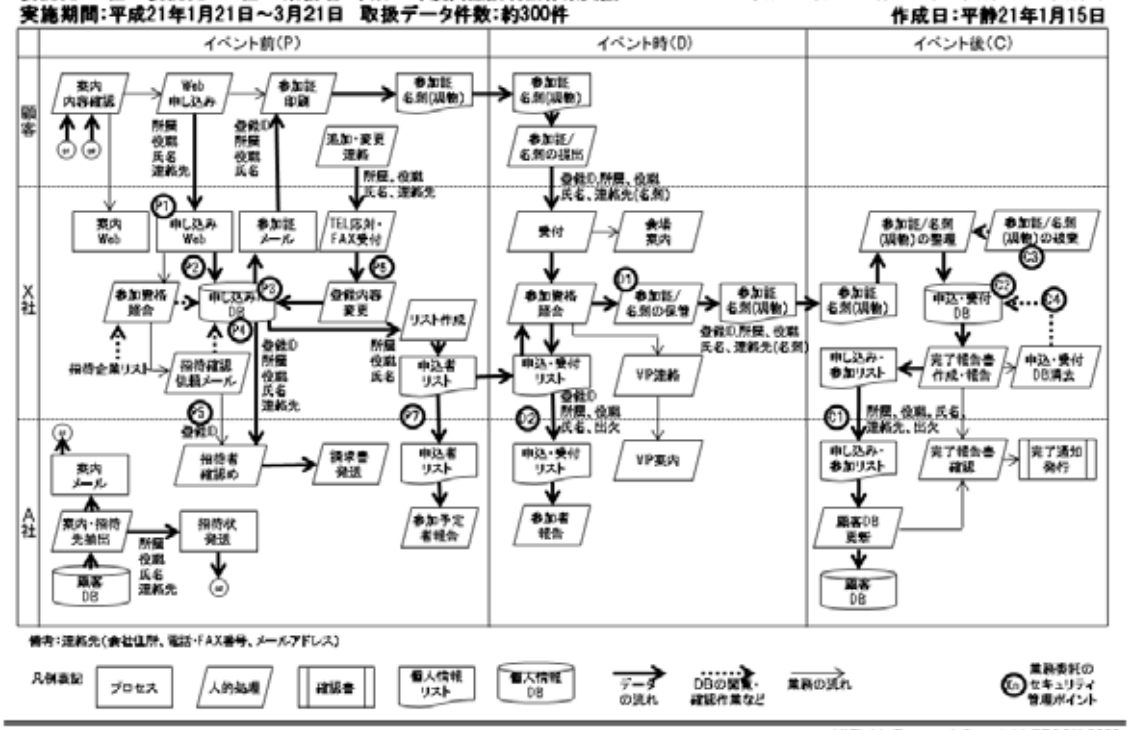


図 商品説明会の作業内容

草案　　例題

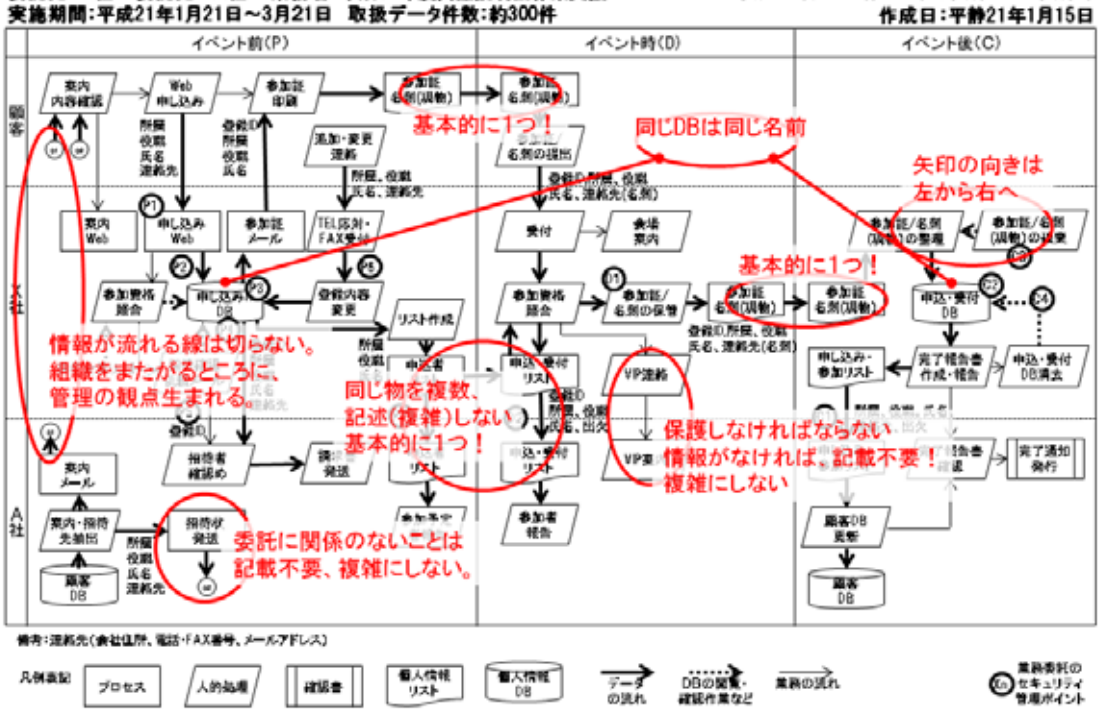
委託元：A社　委託先：X社　業務名：平成20年度商品説明会作業支援
実施期間：平成21年1月21日～3月21日　取扱データ件数：約300件
委託内容：Web作成、申込受付、当日受付等
作成日：平静21年1月15日



図作成の注意点　　例題

委託元：A社　委託先：X社　業務名：平成20年度商品説明会作業支援
実施期間：平成21年1月21日～3月21日　取扱データ件数：約300件

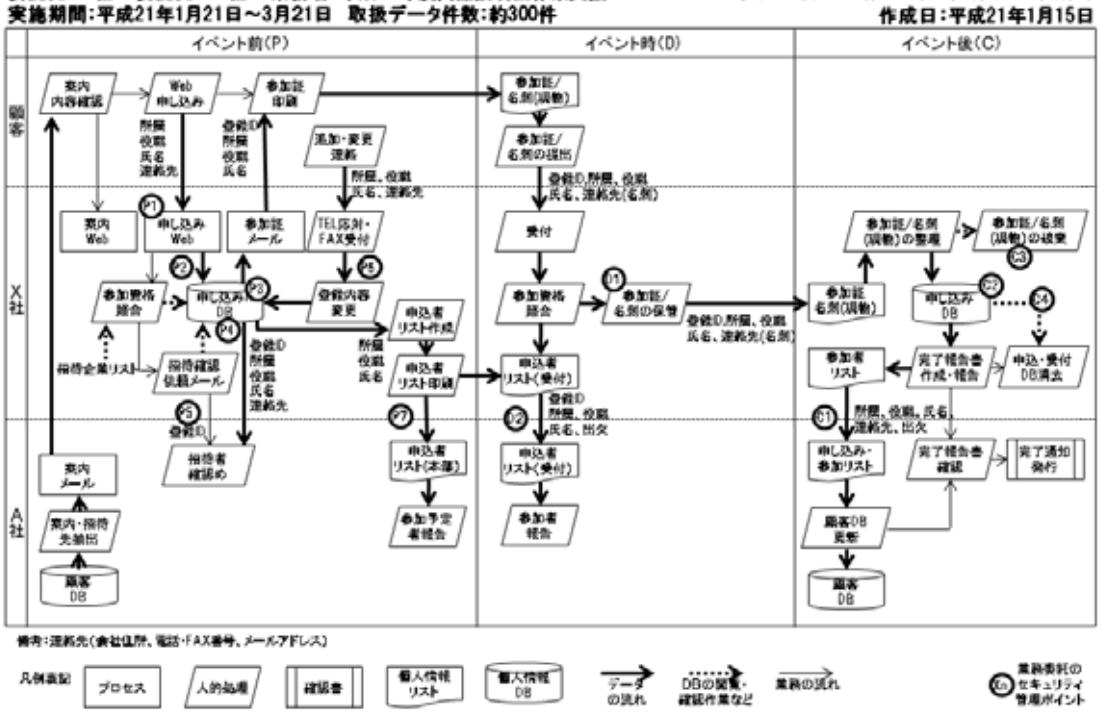
委託内容：Web作成、申込受付、当日受付等
作成日：平静21年1月15日



最終形　　例題

委託元：A社　委託先：X社　業務名：平成20年度商品説明会作業支援
実施期間：平成21年1月21日～3月21日　取扱データ件数：約300件

委託内容：Web作成、申込受付、当日受付等
作成日：平成21年1月15日



3. 利用　　例題

(1)委託先の適切選定

■企業の情報保護の調査票の例

情報保護に関し、御社の措置について、下記設問にご回答ください。

企業名[　　] 役職[　　] 回答者氏名[　　印]

Ⅰ. 該当項番に○をし、必要事項を記入ください。
1. プライバシーマーク取得企業(登録番号:　　)
2. ISMSの認証企業(認証範囲:　　)

Ⅱ. 現在の実施状況の該当項番に○を記入してください。
1. 対象者に個人情報保護の教育が行われ、全員が誓約している
2. 個人情報の保護方針があり、ホームページ等で公開している
3. 個人情報の収集に、目的の通知と収集の同意を得ている
4. 保有する個人情報が特定され、管理されている
5. 情報管理者および責任者が定められている

6. 作業場所の入退室管理が行われている
7. 情報保管庫が施錠管理されている
8. 情報のアクセス制限がされている
9. 情報授受に際し、安全対策が施されている
10. 情報授受の記録がとられている

11. 情報管理に関する監査が行われている
12. 情報管理に対する相談窓口がある
13. 情報保護に関する法令及びその他の規範が特定されている
14. 外部委託の際は、機密保持契約を締結している
15. 過去において情報漏えいの事故を起こしたことがない

以上

■本委託内容の情報保護計画の調査票の例

添付の業務データプロセス図により担当業務おける情報の流れを確認し、下記の情報保護について記入してください。

企業名[　　] 部署名[　　] 氏名[　　印]

Ⅰ. イベント前(P)
P1:申し込みWebに個人情報を保護する安全措置を取るか
　>1. 正しいSSL※1、2. ID・パスワード、3. その他(　　)、4. しない
P2:申し込みDBに外部からの不正アクセスを防止するか
　>1. 正しいWebAP※2、ファイヤーウォール、3. その他(　　)、4. しない
P3:申し込みDBのアクセス許可管理をするか
　>1. ICカード、2. ID・パスワード、3. その他(　　)、4. しない
P4:申し込みDBのアクセス履歴をとるか
　>1. 全データ、2. アクセスID・ファイル名、3. その他(　　)、4. しない
P5:弊社への連絡は必要最低限情報であることを考慮するか
　>1. 考慮する、2. 考慮しない
P6:TEL応対・FAX受付などでの情報、現物の管理をするか。
　>1. 台帳管理、2. アクセス者限定、3. その他(　　)、4. しない
P7:申込者リスト(現物)の受け渡しを管理するか
　>1. 台帳管理、2. アクセス者限定、3. その他(　　)、4. しない
Ⅱ. イベント時(D)
D1:会場での参加証/名刺(現物)の保管の管理をするか
　>1. 台帳管理、2. 取扱者限定、3. その他(　　)、4. しない
D2:会場での申込・受付リストの受け渡しの管理をするか
　>1. 台帳管理、2. 受渡者限定、3. その他(　　)、4. しない
Ⅲ. イベント後(C)
C1:申込・受付リストの受け渡し方法を管理するか
　>1. 暗号メール、2. 手渡し、3. その他(　　)、4. しない
C2:申込・受付DBのアクセス管理をするか
　>1. ICカード、2. ID・パスワード、3. その他(　　)、4. しない
C3:参加証/名刺(現物)破棄の確認をするか
　>1. 台帳との確認、2. アクセス者確認、3. その他(　　)、4. しない
C4:申込・受付DB消去の確認をするか
　>1. 台帳との確認、2. アクセス者確認、3. その他(　　)、4. しない

注意:
※1、※2: ECOM成果報告書:ECにおける情報セキュリティに関する活動報告書2008、ppXX1-YY1,XX2-yy2を参照のこと
御社との委託契約が成立した場合には、本調査票を御社との機密保持契約書に添付します。予めご承知置き下さい。

例題

(2)必要な契約の締結

■業務委託契約書

ABC株式会社(以下「甲」という。)と株式会社XYZ(以下「乙」という。)とは、次の通り契約を締結する。
第1条(委託)
甲は第2条1号に定める業務内容に関する作業「以下「本作業」という。」を同条第2号以下に定める要領により、乙に作業を依頼する。
第2条(業務内容)
業務委託内容は次の各号の通りとする。
　業務名　:平成20年度商品説明会作業支援
　作業内容:本契約書添付の作業計画書
　契約期間:平成21年1月21日から平成21年3月21日まで
第3条(再委託)
乙は本作業を作業計画書に記載された計画に従って実施するものとし、甲の承諾無く本作業の全部または一部を第三者に・・・
第4条(営業秘密)
乙は甲の承諾無しに本作業に関わる一切の事項を第三者に漏洩しないものとし、**本契約書添付の情報保護計画書に基づき作業を行うものとする。**本契約終了後も同様とする。
第5条(知的所有権)
第6条(完了報告)
乙は作業計画書および**情報保護計画書に基づき**実施した作業の結果を、平成21年3月30日までに甲に報告するものとする。
第7条(監査事項)
甲は、本作業完了1年以内に、乙に対し**関係書類その他必要な資料**を提出させて監査を行うことができるものとする。
第8条(期間延長)、第9条(契約金額と支払)、第10条(遅滞損害金)
第11条(権利譲渡)、第12条(免責事項)、第13条(契約費用)
第14条(定めなき事項)、第15条(信義誠実)

平成21年1月20日
甲　東京都港北区あいう1丁目2番3号　ABC 株式会社　調達部
　　部長　日本 太郎
乙　東京都港東区かきく1丁目2番3号　株式会社XYZ
　　代表取締役社長　東京 一郎

■本委託内容の情報保護計画の調査結果

添付の業務データプロセス図により担当業務おける情報の流れを確認し、下記の情報保護について記入してください。

企業名[　X社　] 部署名[業務課] 氏名[田中一郎]

Ⅰ. イベント前(P)
P1:申し込みWebに個人情報を保護する安全措置を取るか
　>1. 正しいSSL※1、2. ID・パスワード、3. その他(　　)、4. しない
P2:申し込みDBに外部からの不正アクセスを防止するか
　>1. 正しいWebAP※2、ファイヤーウォール、3. その他(　　)、4. しない
P3:申し込みDBのアクセス許可管理をするか
　>1. ICカード、2. ID・パスワード、3. その他(　　)、4. しない
P4:申し込みDBのアクセス履歴をとるか
　>1. 全データ、2. アクセスID・ファイル名、3. その他(　　)、4. しない
P5:弊社への連絡は必要最低限情報であることを考慮するか
　>1. 考慮する、2. 考慮しない
P6:TEL応対・FAX受付などでの情報、現物の管理をするか。
　>1. 台帳管理、2. 取扱者限定、3. その他(　　)、4. しない
P7:申込者リスト(現物)の受け渡しを管理するか
　>1. 台帳管理、2. 取扱者限定、3. その他(　　)、4. しない
Ⅱ. イベント時(D)
D1:会場での参加証/名刺(現物)の保管の管理をするか
　>1. 台帳管理、2. 取扱者限定、3. その他(　　)、4. しない
D2:会場での申込・受付リストの受け渡しの管理をするか
　>1. 台帳管理、2. 受渡者限定、3. その他(　　)、4. しない
Ⅲ. イベント後(C)
C1:申込・受付リストの受け渡し方法を管理するか
　>1. 暗号メール、2. 手渡し、3. その他(　　)、4. しない
C2:申込・受付DBのアクセス管理をするか
　>1. ICカード、2. ID・パスワード、3. その他(　　)、4. しない
C3:参加証/名刺(現物)破棄の確認をするか
　>1. 台帳との確認、2. アクセス者確認、3. その他(　　)、4. しない
C4:申込・受付DB消去の確認をするか
　>1. 台帳との確認、2. アクセス者確認、3. その他(　　)、4. しない
以上

業務データプロセス図による情報保護の展開　例題

(3)取扱状況の把握(委託先の監督)

■本委託内容の情報保護計画の調査票

添付の業務データプロセス図により担当業務おける情報の流れを確認し、
下記の情報保護について記入してください。
企業名[　X社　] 部署名[業務課] 氏名[田中一郎]

Ⅰ. イベント前(P)
P1:申し込みWebに個人情報を保護する安全措置を取るか
　>1. 正しいSSL※1、2. ID・パスワード、3. その他(　　)、4. しない
P2:申し込みDBに外部からの不正アクセスを防止するか
　>1. 正しいWebAP※2、2. ファイヤーウォール、3. その他(　　)、4. しない
P3:申し込みDBのアクセス許可管理をするか
　>1. ICカード、2. ID・パスワード、3. その他(　　)、4. しない
P4:申し込みDBのアクセス履歴をとるか
　>1. 全データ、2. アクセスID・ファイル名、3. その他(　　)、4. しない
P5:弊社への連絡は必要最低限情報であることを考慮するか
　>1. 考慮する、2. 考慮しない
P6:TEL応対・FAX受付などでの情報、現物の管理をするか。
　>1. 台帳管理、2. 取扱者限定、3. その他(　　)、4. しない
P7:申込者リスト(現物)の受け渡しを管理するか
　>1. 台帳管理、2. 取扱者限定、3. その他(　　)、4. しない
Ⅱ. イベント時(D)
D1:会場での参加証/名刺(現物)の保管の管理をするか
　>1. 台帳管理、2. 取扱者限定、3. その他(　　)、4. しない
D2:会場での申込・受付リストの受け渡しの管理をするか
　>1. 台帳管理、2. 受渡者限定、3. その他(　　)、4. しない
Ⅲ. イベント後(C)
C1:申込・受付リストの受け渡し方法を管理するか
　>1. 暗号メール、2. 手渡し、3. その他(　　)、4. しない
C2:申込・受付DBのアクセス管理をするか
　>1. ICカード、2. ID・パスワード、3. その他(　　)、4. しない
C3:参加証/名刺(現物)破棄の確認をするか
　>1. 台帳との確認、2. アクセス者確認、3. その他(　　)、4. しない
C4:申込・受付DB消去の確認をするか
　>1. 台帳との確認、2. アクセス者確認、3. その他(　　)、4. しない
以上

■情報保護計画の実施状況報告

添付の業務データプロセス図により担当業務おける情報の流れを確認し、
下記の情報保護の実施状況を記入してください。
企業名[　X社　] 部署名[業務課] 氏名[田中一郎]　記載日[3月15日]

Ⅰ. イベント前(P)
P1:申し込みWebに個人情報を保護する安全措置
　>1. 正しいSSL※1　<正しいサーバー証明書※1にて実施
P2:申し込みDBに外部からの不正アクセス防止
　>1. 正しいWebAP※2　<正しいWebAP※2にて実施
P3:申し込みDBのアクセス管理をするか
　>2. ID・パスワード　<弊社:4名に発行、貴社:2名に発行
P4:申し込みDBのアクセス履歴
　>2. アクセスID・ファイル名　<不正アクセスなし
P5:弊社への連絡は必要最低限情報であることを考慮するか
　>1. 考慮する　<基本的に登録IDのみとした。
P6:TEL応対・FAX受付などでの情報、現物の管理をするか。
　>1. 取扱者限定　<弊社:4名に限定
P7:申込者リスト(現物)の受け渡しを管理するか
　>2. 取扱者限定　<貴社:鈴木二郎様のみ
Ⅱ. イベント時(D) 3月16日
D1:会場での参加証/名刺(現物)の保管の管理をするか
　>2. 取扱者限定　<弊社:田中一郎、山本裕子(予定)
D2:会場での申込・受付リストの受け渡しの管理をするか
　>2. 受渡者限定　<貴社:鈴木二郎様、佐藤浩子様(予定)
Ⅲ. イベント後(C)
C1:申込・受付リストの受け渡し方法を管理するか
　>2. 手渡し　<完了報告時の予定
C2:申込・受付DBのアクセス管理をするか
　>2. ID・パスワード　<田中PCにて確認完了まで保管の予定
C3:参加証/名刺(現物)破棄の確認をするか
　>2. 取扱者確認　<
C4:申込・受付DB消去の確認をするか
　>2. 取扱者確認　<
Ⅳ. 懸念事項
　<不達 郵便(12、123、345)、メール(23、345)　・・・　以上

例題

(4)お客様へのアナウンス

お得意様各位

東京都港北区あいう1丁目2番3号
ABC 株式会社

平成21年度 新商品説明会のご案内

1. 日　時 ： 平成21年3月15日(金)　13:30ー16:50
2. 場　所 ： 昭和記念館
3. プログラム ：
　13:30 ・ 新春モデルのご紹介
　15:30 ー ご商談会

4. お申込み内容:

会員区分:	特約店・一般
企業・団体名	
参加者名: (役職)	
連絡先	住所: TEL:　　fax: E-Mail:
個人情報取扱いについて	□下記の個人情報の取扱い □同意しない。(この場合参加

※ 個人情報の取扱いについて
・「参加申込書」に記載された個人情報は、本行事の運営管理のために使用します。

・本行事の参加申込み受付、当日の運営等の業務を外部に委託して実施する場合があります。

・外部委託する場合には、当社は業務委託先が個人情報を適切に運営管理しているかを監督します。

・業務委託先以外の第三者への個人情報の提供・開示は行いません。
・本行事の終了後、個人情報は速やかに破棄します。
・申込みご本人からの個人情報に関する開示または訂正、削除の請求があった場合、該当個人情報の申込みご本人への開示、または訂正、削除します。

※ 個人情報の取扱いについて
・「参加申込書」に記載された個人情報は、本行事の運営管理のため
・本行事の参加申込み受付、当日の運営等の業務を外部に委託して
あります。
・外部委託する場合に、当社は業務委託先が個人情報を適切に運営
監督します。
・業務委託先以外の第三者への個人情報の提供・開示は行いません。
・本行事の終了後、個人情報は速やかに破棄します。
・申込みご本人からの個人情報に関する開示または訂正、削除の請
該当個人情報の申込みご本人への開示、または訂正、削除します。

アンケート 1/4

1. 利用について

BDPC：業務データプロセスチャート

(1)企業間で共通認識を得るためにBPDCと同等の図を使っている。

□使っている □使っていない □わからない

利用シーン(自社内の共通認識、委託先選定、契約、監督、監査など):

・

(2)BPDCを業務委託契約書に添付することについて

□大変良い □よい □どちらでもない □よくない □大変悪い

理由:

・

(3)BDPCを委託先の選定に利用することについて

□大変良い □よい □どちらでもない □よくない □大変悪い

理由:

・

(4)BDPCを委託先の監督に利用することについて

□大変良い □よい □どちらでもない □よくない □大変悪い

理由:

・

13

アンケート 2/4

2. 記載内容について

(1)BDPCの記述内容(データの発生から消滅までのプロセス(取扱の要求定義)のみを記述する)について

□大変良い □よい □どちらでもない □よくない □大変悪い

理由:不要・不足な記述内容など

・

(2)BDPCの記述内容(情報セキュリティに対する装置、システム、機能を記述しない)について

□大変良い □よい □どちらでもない □よくない □大変悪い

理由:不要・不足な記述内容など

・

(3)BDPCの作成で使用する記号(表記方式)について

□大変良い □よい □どちらでもない □よくない □大変悪い

理由:不要・不足な記号など

・

(4)BDPCの作成で参考となる例(基本例のみ)について

□大変良い □よい □どちらでもない □よくない □大変悪い

理由:再委託、3者間、複数間委託時についてなど

・

14

アンケート 3/4

3. 普及について

(1)自社内や委託業務でBDPCによる共通理解の推進について

□実施する □実施したい □検討する □わからない □実施しない

理由:

・

(2)BDPCの表記方式の標準化について

□大変良い □よい □どちらでもない □よくない □大変悪い

理由:実現すべき標準化のレベル:政府ガイドライン、ECOMガイドライン、ガイド(推奨)、報告程度

・

(3)業務データプロセスチャートという名前について

□大変良い □よい □どちらでもない □よくない □大変悪い

理由:その他の名前

・

アンケート 4/E

4. 企業間情報保護連携(SWG1)の来年度の活動について

(1)BDPCによる共通理解の普及について

□大変良い □よい □どちらでもない □よくない □大変悪い

意見:

・

(2)企業間情報保護連携で来年度実施すべきテーマについて

意見:

・

(3)安全・安心EC環境整備として来年度実施すべきテーマについて

意見:

・

付録 B-2 アンケート回答

(回答者：A,B,C,D,E)

1. 利用について

(1) 企業間で共通認識を得るためにＢＰＤＣと同等の図を使っている。

■使っている D、■使っていない A、E、■わからない C

利用シーン：

D.BDPC：業務データプロセスチャートという名称及び P.8 のようなフォーマットではありませんが守るべき技術情報または個人情報について、情報のやり取りを 1 枚の紙にまとめは実施している

(2) ＢＰＤＣを業務委託契約書に添付することについて

■大変良い C、よい E、■どちらでもない A, D、□よくない、□大変悪い

理由：

D.業務委託契約書の内容によるのでどちらとも言えない。

E. 多分、あった方が良いのだと思います。

(3) ＢＤＰＣを委託先の選定に利用することについて

■大変良い C、■よい D、■どちらでもない A、E、□よくない、□大変悪い

理由：

D.選定する際、守るべき資産がどのような範囲で動くのかリスクが明確になるので、遵守すべきセキュリティレベルに応じた業者を選定する必要があるので、あったほうがよい。判断材料になる。

E. どう利用するのでしょうか？選定作業の流れでしょうか？

(4) ＢＤＰＣを委託先の監督に利用することについて

■大変良い C、■よい D、■どちらでもない A、E、□よくない、□大変悪い

理由：

D.良いというよりは個人情報を取り扱い管理・監督の義務が発生するので、必要である。

2. 記載内容について

(1) ＢＤＰＣ記述内容(データの発生から消滅までのプロセス(取扱の要求定義)のみを記述する)について

■大変良い C、■よい A、D、E□どちらでもない、□よくない、□大変悪い

理由：

D.書き方の表現はいろいろありますが、データの発生から消滅までのやり取りを明確化することは必要である。

E. 組織的な情報管理の姿として、1 つの方向だと思います

(2) ＢＤＰＣの記述内容 (情報セキュリティに対する装置、システム、機能を記述しない) について

■大変良い C、■よい A、■どちらでもない E、■よくない D、□大変悪い

理由:

D.システムの機能に関しては BDPC とは別で整理したほうがよい。
あくまでも BDPC はデータのプロセスのみ明記する。

E. 他のドキュメントで補完できるならそれでも良いのでしょう。面倒かも。

⑶ ＢＤＰＣの作成で使用する記号（表記方式）について

■大変良い A、C、□よい、■どちらでもない D、E、□よくない、□大変悪い

理由:

⑷ ＢＤＰＣの作成で参考となる例（基本例のみ）について

□大変良い、□よい、■どちらでもない A、C、D、E、□よくない、□大変悪い

理由:再委託、三者間、複数間委託時についてなど

D.

・再委託を許可した場合複雑化すぎる。

・このフォーマットに決めてしまうと、再委託、複数者の業者へ委託する場合書けない。

・1 枚に複数業者を書く場合、どこまでオープンにするかなどよく考えないといけない。

E. 適当な雛形が無いと、新しい取り組みをしたがらないのでは？

3. 普及について

⑴ 自社内や委託業務でＢＤＰＣによる共通理解の推進について

■実施する D、□実施したい、■検討する E、■わからない A、C、□実施しない

理由:

D.同じフォーマット、ルールではないが、社内の基準に従い、既に行っている。

E. まともな組織を考えるなら、検討対象の 1 つだと思います。

⑵ ＢＤＰＣの表記方式の標準化について

□大変良い、□よい、■どちらでもない A、C、E、■よくない D、■大変悪い

理由:実現すべき標準化のレベル:政府ガイドライン、ＥＣＯＭガイドライン、ガイド（推奨）、報告程度など

A.まずは報告程度を目標とし、コンセンサスの範囲、度合いに応じて
標準化のレベルをグレードアップする方法も考えられる。

C.推奨にとどめておき、詳細は各社様式を定めればよいと思います。

D.今段階でわざわざ標準化レベルまでする必要はないのではないか？
QMS という基準があり、その図を活用すれば標準化になるのではない？

E. とりあえず、自由にやらせてみては

⑶ 業務データプロセスチャートという名前について

□大変良い、■よい A、■どちらでもない D、E、■よくない C、□大変悪い

理由:その他の名前

C.業務データのうち保護対象のみ記載するので、単に業務データとしない。

D.特になし

機密情報及び個人情報のみに実施させるのであれば、BDPC ではないような気がします。すべての「EC における企業間情報保護連携」という範囲で課すのであればこの名前でも良いかと思います。

4. 企業間情報保護連携（SWG1）の来年度の活動について

（1）BDPC による共通理解の普及について

□大変良い、■よい A、D、E、■どちらでもない C、□よくない、□大変悪い

意見:

B.共通理解はよいのですが、普及させるには「普及版」が必要ではないかとおもいます。
今年度のフローで中小企業に普及させるには、予算、人員でかなりむりがあると思う。
導入に必要な条件の検討と表示が必要かと。
できれば、他のソリューションとの比較表の添付など。

D.普及することについてはよいと思う。

（2）企業間情報保護連携で来年度実施すべきテーマについて

意見:

・費用の少ない普及版の検討
・具体的な情報のモデル（種類：CAD、個人情報、会計情報）を使った研究？

（3）安全・安心 EC 環境整備として来年度実施すべきテーマについて

意見:

・最近多くの企業や団体で検討が始まっている「秘密分散技術」を利用したセキュリティ。「電子割符」を用いた安全・安心技術に関するテーマ
・もっと実社会との連携を密接に感じられる情報システムとのインターフェースや、認証、セキュリティシステムの必要性の調査

以上

業務データプロセスセキュリティ評価チャート (BDPS EC)

■目的

・顧客情報などの情報保護を必要とする機密データに対する処理のプロセスを明確化する図である。
・作業委託を行なう場合、①委託先の適切な選択、②委託先との契約、③取り扱い状況の把握において、委託先と委託元で、情報保護を行なうべき管理ポイントの共通認識を得る図である。

■特徴

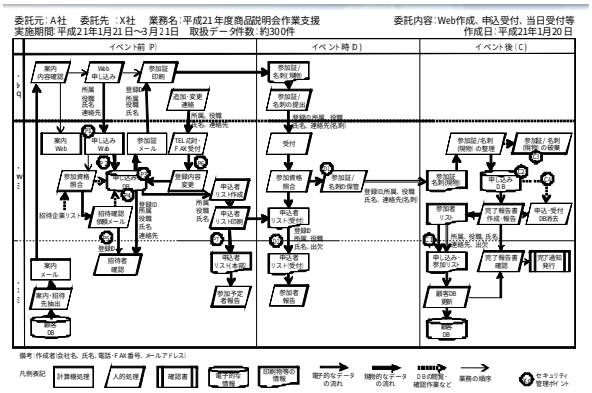
・処理のプロセスだけを分離記述する。実施手段 (計算機、ネットワーク) は記載しない。
・保護を必要とするデータを中心として記述し、保護を必要としないデータは記述しない。

■記述形式

・図の縦軸は組織、横軸は時系列 (処理の流れが変わるフェーズごとに記述分割する)。
・機密データの発生から消滅までの処理のフローを下記の記号を用いて記述する。

計算機処理	データ編集などの計算機処理
人的処理	データ加工などの人的処理
確認書	データ編集・加工の確認
データ (印刷物)	印刷物 (現物) によるデータ
電子的格納 DB	DB格納などにとるデータ
⟹	データの流れ (現物、紙など)
⟹	データの流れ (電子的、メール他)
⟶	業務の流れ
⋯⋯→	情報の閲覧・確認作業など
Ⓐ	情報保護の管理ポイント

2. BDP SEC 作成例



BDPS EC ワークシート

委託元：　社　委託先：　社　業務名：　　委託内容：
実施期間：平成21年　月　日～　月　日　　取扱データ件数：　　件　　作成日：　　年　月　日

	実施前 (P)	実施時 (D)	実施後 (C)
情報主体			
社			
社			

備考：連絡先 (会社住所、電話・FAX番号、メールアドレス)

凡例表記　計算機処理　人的処理　確認書　電子的な情報　印刷物等の情報　電子的なデータの流れ　現物的なデータの流れ　DBの閲覧・確認作業など　業務の順序　Ⓐ セキュリティ管理ポイント

3. Web セキュリティ SWG 活動報告

はじめに

インターネットを介して消費者が事業者から物品やサービスを購入する消費者向けの電子商取引(以下 EC)は、IT 技術の進歩に伴って年々市場規模を拡大している。

消費者は、パソコン（以下 PC）に代表される端末を利用して一般的に Web で構成される EC サイトから物品、サービスを購入する。この際に、端末で動作するブラウザソフトと EC サイトである Web サイトとの間でインターネットを介した通信を行い、電子商取引を実現させる。この取引を成立させるためには、消費者は自らの個人情報（住所、氏名、電話番号、生年月日、性別、カード番号、銀行口座など）を Web サイトに送信する必要があるし、Web サイトはログインしている消費者が正しく認証されたユーザーであることを確認する必要がある。

このような処理を保障する安全・安心の仕組みは、一般的には技術および運用上の仕組みにより確保可能となる。しかしながら、Web2.0 に代表される近年の Web 技術の急速な進歩に現場のセキュリティ対策が追いついていない事情があることや、ハッカー、クラッカーと呼ばれる攻撃者の攻撃手法が組織犯罪化し、ブラックビジネス化していることなどの事情で Web サイト運営者側の脅威は高まっている。

また、端末側も PC 以外に、携帯電話、スマートフォン、TV 等の情報家電など種々のものが登場しており、機能向上の反面、利用者操作の複雑さが増したり、個人情報売買やなりすまし等の犯罪行為に巻き込まれるなどのトラブルも増加している。

このような状況を鑑み、ECOM EC 安全・安心グループの情報セキュリティ WG のサブワーキング（SWG2）として、Web セキュリティ課題検討・普及啓発を本 SWG のテーマにとりあげた。

本 SWG では、今年度は調査活動として位置づけ、電子商取引の実態と Web セキュリティの現状を事例収集し、実態をまとめた。今回の事例収集は Web セキュリティの調査ではあるが、現場レベルでは Web セキュリティに関わる脅威が発生する原因を探っていくと管理不徹底などのバックグラウンド事情が必ず存在するものであり、また最初は全体を把握する目的もあるため、Web セキュリティに直接は関わらないがなんからの関連があると思われる事例も収集している。このため、収集事例は広く浅くの傾向で収集されている。

最終的にガイドラインを策定するためには、対象と目的を絞ったさらなる調査を必要なら複数種類で実施すべきである。

3.1. 電子商取引とWebセキュリティの現状

経済産業省の「平成 18 年度電子商取引に関する市場調査」によると、2006 年度の日本における B to C－EC 市場規模は、4 兆 3910 億円であるとされる。1998 年頃から米国発の大手 EC サイトを中心として PC、書籍・CD などの購入から始まった EC は、ADSL などブロードバンド普及が始まった 2001 年頃から提供者、利用者ともに裾野が広がっていった。

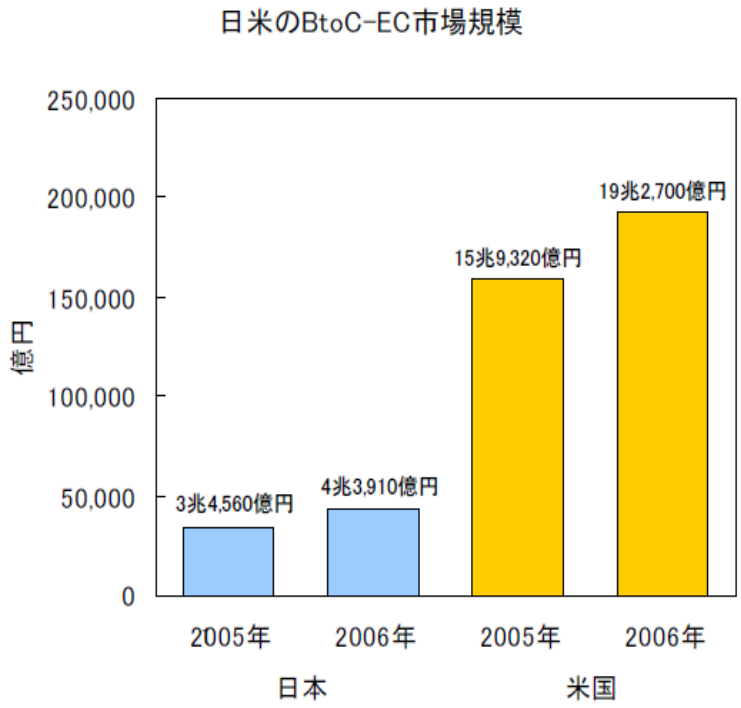


図 3.1　日本における B to C－EC 市場規模

経済産業省「平成 18 年度電子商取引に関する市場調査」より

具体的には、楽天、Yahoo!などが主催するインターネットモールへの中小ショップの参画、消費者同士のオークションの定着や、Amazon などでの利用者購入履歴から類推してリコメンド商品を提示するような付加価値サービスの提供、価格比較サイトを活用した安値提供の中小ショップおよび価格比較サイトを積極利用する消費者の存在などがあげられる。また、端末も PC だけでなく、携帯端末の機能（メール、アプリ）、通信速度向上に伴って、着メロ、着歌、楽曲・動画・小説など携帯向けモバイルコンテンツも大幅に発展してきている。

さらに最近では、ブログ、SNS（***Social Networking Service***）に代表される CGM（Consumer Generated Media）が発達し、ブログ、口コミを中心に価格だけでなく納期、送料、アフターサービスなど全般の評価が EC ショップ選定で重要になりつつある。

また、ブログを利用したアフェリエイト、ドロップシッピングなど、消費者が単に消費する立場から、発信し積極的に購買を支援する立場に変化してきていることも見逃せない。図 3.2 に EC サイトの例を示す。

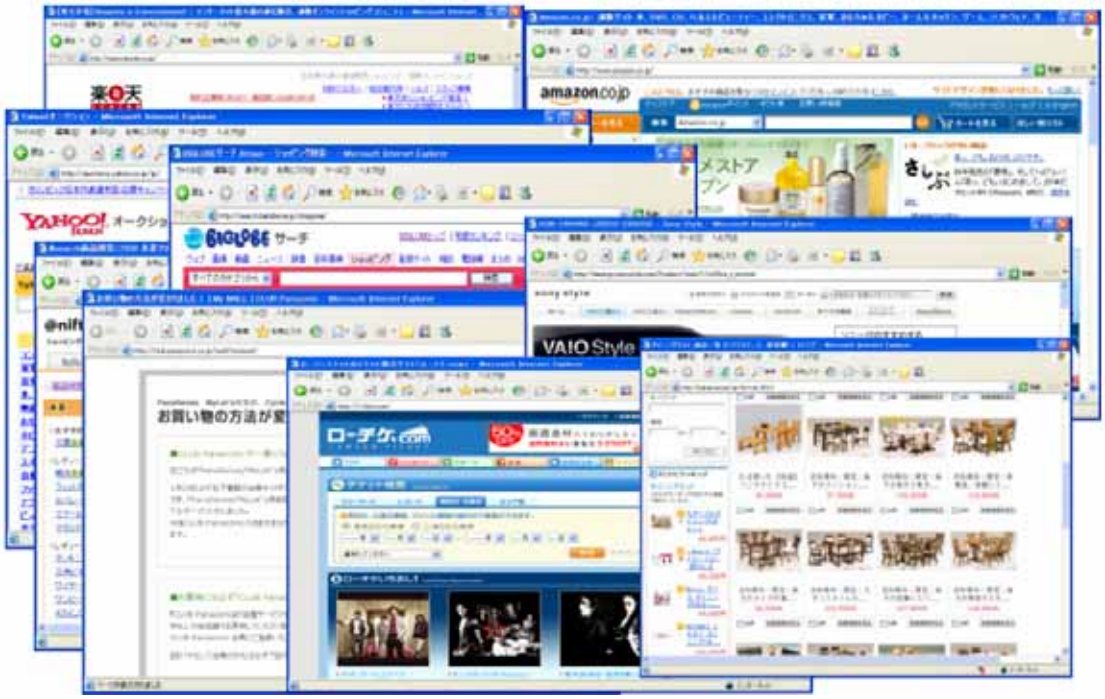


図 3.2　EC サイトの例

また、消費者が利用する端末についても、当初は PC、コンビニ等の専用端末だけであったが、携帯電話において

1）CDMA 1X WIN、HSDPA 等第 3.5 世代携帯電話（3.5G）通信開始されたこと

2）ハード、ソフト面での大幅な機能の向上がなされたこと

例）i モード、i アプリなどの携帯アプリ進歩、フルブラウザの搭載、

QR コードとカメラ機能連動によるサイト URL への自動アクセス

おサイフ携帯など決済機能つき携帯電話等々

3）着メロ、着歌、楽曲販売、携帯小説、ゲーム、SNS などのサービスの進化

などの発展があり、主に若年層対象とした各種携帯 EC サイトが盛んになっており、携帯電話が EC 端末として重要な位置を占めるに至っている。

図 3.3 に各キャリアの携帯サービスの例を示す。また、図 3.4 にモバイル携帯サイトの例を示す。

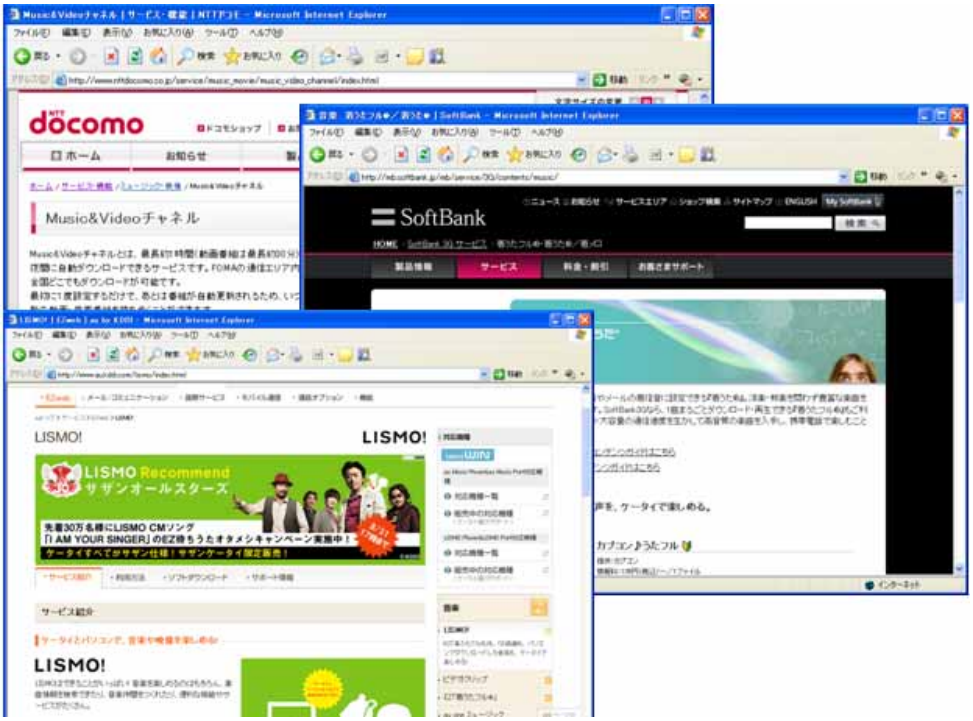


図 3.3 各キャリアの携帯サービスの例

図 3.4 モバイル携帯サイトの例

さらに最近では、TV など情報家電も EC の端末として利用可能となっている。例えば、パナソニック株式会社、ソネットエンタテインメント株式会社、ソニー株式会社、シャープ株式会社、株式会社東芝、株式会社日立製作所で出資しているアクトビラ社は、上記 TV 製造会社 5 社のインターネット接続機能つき TV に対して、インターネットコンテンツを提供している。図 3.5 にアクトビラ社の HP を示す。

図 3.5 アクトビラ社 HP

2008 年 8 月現在アクトビラサービス上では、楽天株式会社が運営している楽天市場で物品の購入が可能である。(但し、購入は TV 上に表示される QR コードを利用した携帯での注文となる) またアクトビラ社および株式会社 TSUTAYA は、アクトビラ上で動画販売を行っており、映画などのコンテンツをダウンロードして TV 上で視聴できる。

図 3.6 アクトビラ上の動画販売画面

またゲーム機の進歩も著しく、ワイヤレス LAN 機能などを備えた機種ではゲーム機から直接ゲームコンテンツ販売サイトにアクセスして、ゲームコンテンツをダウンロードできるサービスの展開予定があるものもある。これにより、親機や PC を経由せずにゲームコンテンツ等を手

軽にダウンロードできる。

以下に、ソニー製ゲーム機の主な仕様を示す。

商品名称 PSP®「プレイステーション・ポータブル」
CPU PSP CPU（動作周波数 1～333MHz）
メイン・メモリ 64MB
ディスプレイ 4.3 インチ 16:9 ワイドスクリーン TFT 液晶
480 x 272 ピクセル 1,677 万色
サウンド ステレオスピーカー内蔵
主な I/O ワイヤレス LAN （IEEE 802.11b 準拠）(Wi-Fi)
High Speed USB (USB2.0 準拠) (mini-B)メモリースティック PRO デュオ™
内蔵ドライブ 再生専用 UMD® ドライブ
対応プロファイル PSP®（PlayStation®Portable）Game
UMD®Video
アクセスコントロール リージョンコード、視聴年齢制限（パレンタルロック）
ワイヤレス通信機能 インフラストラクチャーモード

対応コーデック（“ メモリースティック ” 上のコンテンツ）
ビデオ メモリースティックビデオフォーマット
MPEG-4 Simple Profile (AAC LC)
H.264/MPEG-4 AVC Main Profile (AAC LC)
MP4 ファイルフォーマット
MPEG-4 Simple Profile (AAC LC)
H.264/MPEG-4 AVC Main Profile - CABAC のみ- (AAC LC)
および Baseline Profile (AAC LC)
AVI
Motion JPEG (Linear PCM あるいはμ-Lau)

ミュージック メモリースティックオーディオフォーマット
ATRAC3™
ATRAC3plus™
MP3
MP3(MPEG-1/2 Audio Layer3)
MP4(MPEG-4 AAC)
WAVE(Linear PCM)
WMA(Windows Media® Audio 9 Standard のみ)
※本体の設定で WMA の再生を有効にする必要があります。

フォト JPEG (DCF2.0/Exif2.21 準拠)

TIFF
BMP
GIF
PNG

同様に携帯が進化した形として、比較的大きな LCD を搭載し、タッチスクリーン型ユーザーI/F などに特徴のある Apple 社の携帯電話機も、EC サイトである Applestore に直接アクセスして、音楽をはじめとしたコンテンツをダウンロード可能である。以下に Apple 社の iPhone 3G の主な仕様を記す。

Apple 社　iPhone 3G の主な仕様

ディスプレイ
3.5 インチ（対角）ワイドスクリーンマルチタッチディスプレイ
480×320 ピクセル解像度 163 ppi
複数言語および文字の同時表示をサポート
オーディオ
周波数特性: 20Hz～20,000Hz
対応するオーディオフォーマット:
AAC、保護された AAC、MP3、MP3 VBR、Audible (フォーマット 1、2、3)、
Apple Lossless、AIFF、WAV
ユーザー設定が可能な音量制限
ビデオ
対応するビデオフォーマット: H.264 ビデオ：
最高 1.5Mbps、 640×480、毎秒 30 フレーム、H.264 バージョンの Low-Complexity ベースラインプロファイル（最高 160Kbps の AAC-LC）、48kHz、.m4v/.mp4/.mov ファイルフォーマットのステレオオーディオ
H.264 ビデオ：最高 768 Kbps、320×240、毎秒 30 フレーム、最高レベル 1.3 のベースラインプロファイル（最高 160Kbps の AAC-LC）、48kHz、.m4v/.mp4/.mov ファイルフォーマットのステレオオーディオ

MPEG-4 ビデオ：最高 2.5 Mbps、640×480、毎秒 30 フレーム、シンプルプロファイル（最高 160Kbps の AAC-LC）、48kHz、.m4v/.mp4/.mov ファイルフォーマットのステレオオーディオ
カメラ
2.0 メガピクセル
写真へのジオタグ添付
iPhone および他社製アプリケーションと連係
メールの添付ファイルに対応

表示可能なドキュメントのタイプ：

.jpg、.tiff、.gif（画像）

.doc、.docx（Microsoft Word）

.htm、.html（Web ページ）

.key（Keynote）

.numbers（Numbers）

.pages（Pages）

.pdf（Preview、Adobe Acrobat）

.ppt、.pptx（Microsoft PowerPoint）

.txt（テキスト）

.vcf（連絡先）

.xls、.xlsx（Microsoft Excel）

このように世の中で EC は隆盛を極めているが、一方で EC を利用する消費者側では、注文した商品が届かない、注文と違う商品が届いたあるいは注文した覚えのない商品が届くなど様々なトラブル、問題が存在する。また、発注、配達に必要な住所、氏名、電話番号、銀行口座番号、クレジットカード番号などの個人情報が流出したり盗まれたりすることで、なりすましによる不正アクセスや後述する犯罪などに巻き込まれる可能性もある。

公正取引委員会が平成 18 年にまとめた「電子商店街等の消費者向け e コマースにおける取引実態に関する調査報告書」によると、「EC サイト運営事業者の資本金及び従業員数は、資本金 5 億円未満、従業員数 500 人未満の事業者が全体の 8 割程度を占めており、比較的小規模な事業者が多い。電子商店街における取引については、運営事業者は一般的には比較的小規模な事業者が多い一方、少数の運営事業者に取引が集中しており、当該運営事業者の事業規模は比較的大きい状況にある。」ということであり、さらに「取引規模（＝電子商店街内で流通する商品等の総額）からみると、楽天（電子商店街の名称：楽天市場）、Yahoo！（同：Yahoo!ショッピング）、DeNA（同：クラブビッダーズ）の 3 社が上位の運営事業者であり、この 3 社の取引規模だけで電子商店街全体の市場規模の約 9 割を占めている」ということである。

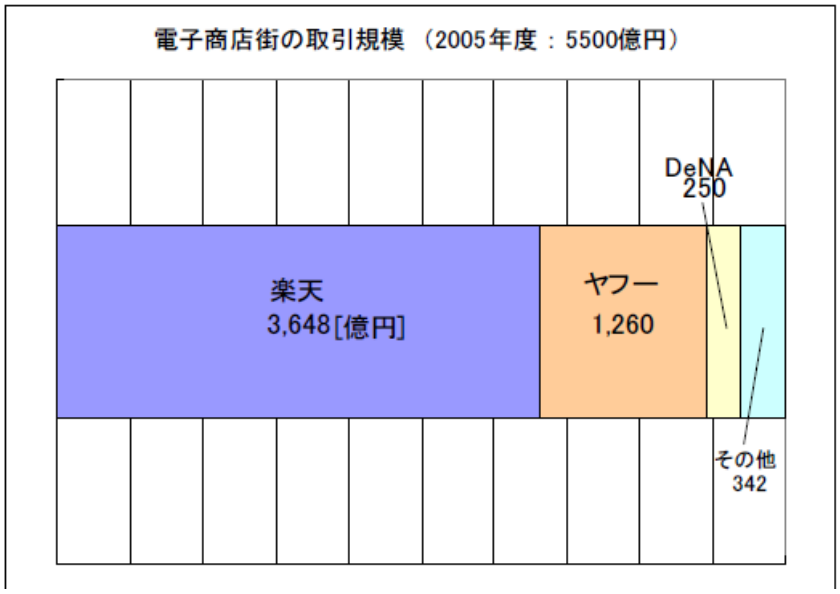


図 3.7 電子商取引における上位 3 社の割合

（公正取引委員会「電子商店街等の消費者向け e コマースにおける取引実態に関する調査報告書」より）

楽天、Yahoo！といった大規模 EC ポータルサイトでは、取引が集中するため上述したような消費者トラブル対応は、初期はともかく経験を積むうちにこなれてくるし、ポータルの親元と出店者との間の契約、ルールなどでの縛り、ノウハウの提供などによりある程度の管理、統制がとられることが期待できると思われる。また、購入画面である Web サイトにしても親元が提供する ASP サービスとなっているので、Web サイト構築、運営は出店者ではなく、親元のポータル運営会社が手がけている。実際、大手ポータル運営会社では図 3.8 に示すように、出店者向けの研修、ガイドラインなどの講座を準備している。

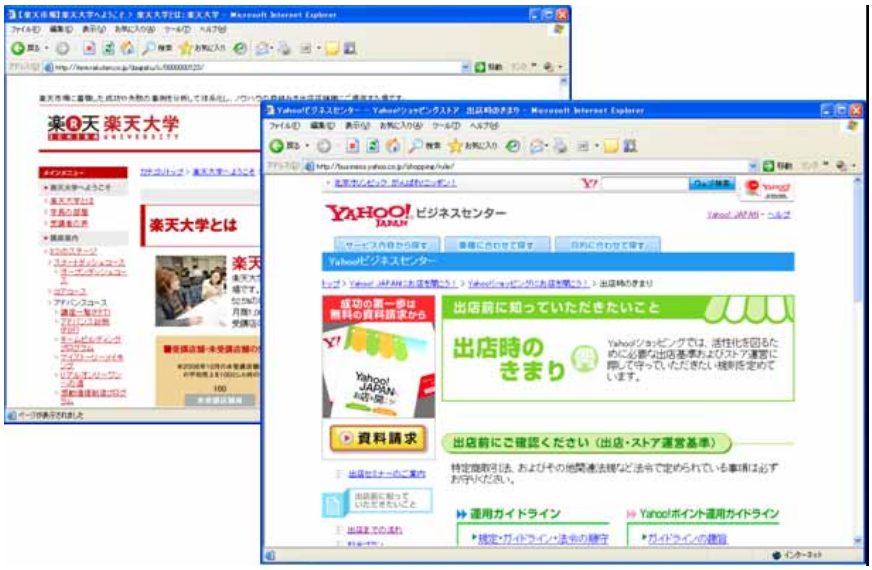


図 3.8 大手ポータルの出店の際の研修、ガイドライン

このように大手ポータル運営会社傘下で出店している EC サイトについては、ある程度の Web セキュリティは保たれると考えられる。このため大手ポータル運営会社に属さずに独自基準で運営している独立系の EC サイトが問題となると思われる。このような EC サイトの運営者は、EC サイトの開発、構築を SIer と呼ばれる開発会社に委託したり、EC サイトの運営は運営会社に委託するのが通常である。

このようなケースでは、EC サイトの要求仕様はサイト運営者が出すにしても、詳細な設計仕様や運用ルールは委託先に丸投げしてしまう例も珍しくない。

本 SWG のテーマは Web セキュリティであり、商品配達に関するトラブルは発注・配達の運用上の問題であるため対象外とすると、EC サイト運営上の課題は、図 3.9 に示すように個人情報を格納している個人情報 DB に関わるところに絞ることができる。なお、決済系の問題は残るが決済系業務については、決済を扱うキャリア系、銀行系、カード会社系などの専門業者に委託するのが一般的であり、EC サイト運営者と彼らとの契約範囲で解決することになり、またこれらの専門業者の回線、設備、運営管理については特殊な専用回線、設備、ルールに基づいて管理されているので本 SWG の対象外とする。

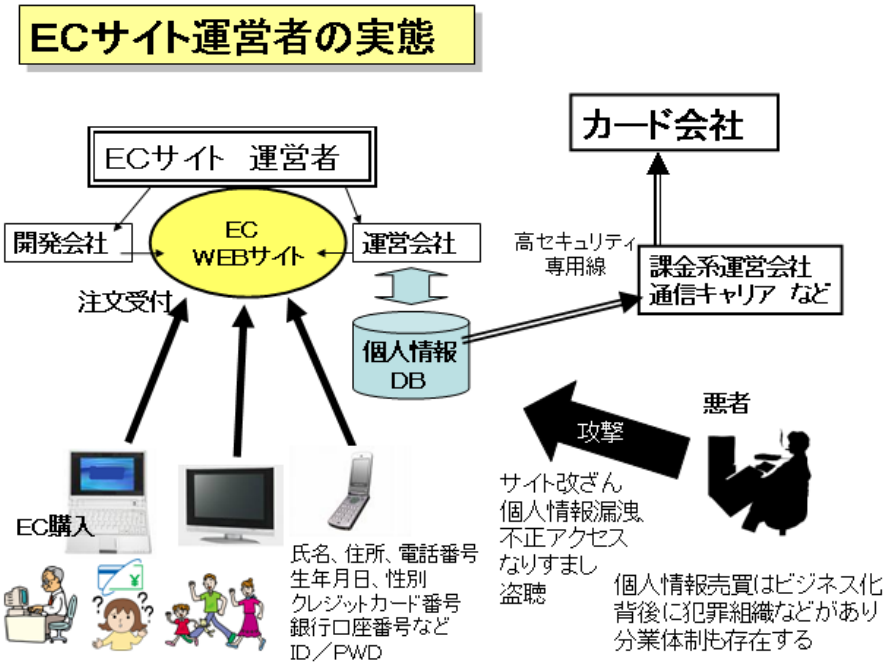


図 3.9 EC サイトの運用実態

次に Web サイトへの攻撃についてであるが、初期の頃はいたずら目的の愉快犯やハッカーなどが自身の技術力の宣伝目的で Web サイトを改ざんしたり、不正アクセスを行ったりしていたが、近年は個人情報の売買目的や政治的理由などで Web サイトを攻撃する例が増えている。

図 3.10 は、IPA（独立行政法人 情報処理推進機構）発行の「情報セキュリティ白書 2007 年版」に掲載されている 2006 年度 10 大脅威の関係である。

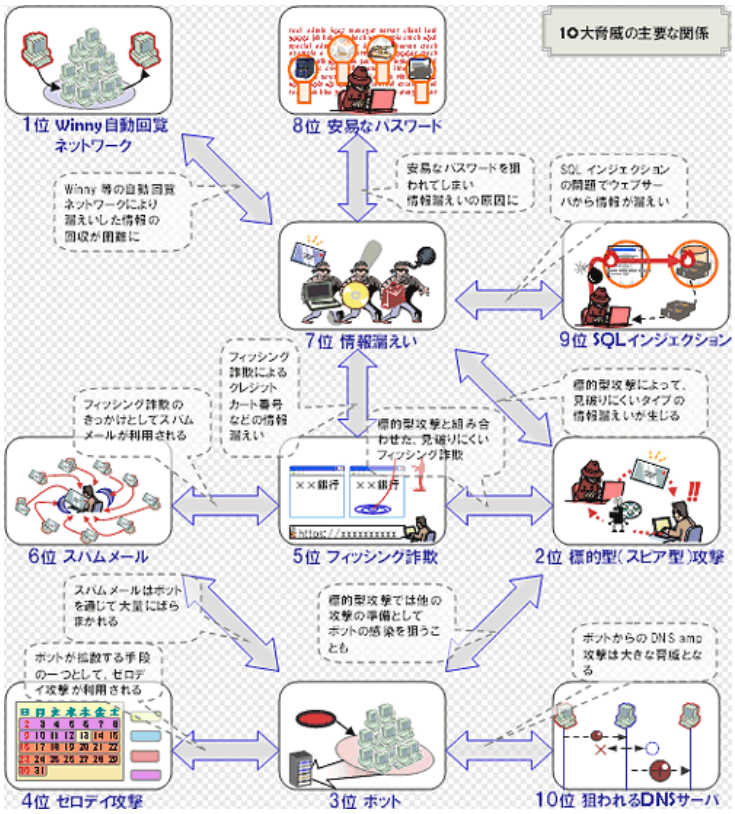


図 3.10 2006 年度 10 大脅威の関係

IPA（独立行政法人 情報処理推進機構）発行「情報セキュリティ白書 2007 年版」より

本白書では、「見えなくなる脅威」と題し、2006 年の傾向として「昨年から引続き情報漏えいは多発しており、減少の傾向は見られません。安易なパスワードを狙った Web システムへの不正侵入や、Web サイトのデータベースを狙った SQL インジェクション攻撃など、攻撃は増え続けており、更に金銭目的化にも拍車がかかっています。また、Winny においては、利用者が意図せず情報流出の被害を拡大させる点が問題になっています。

また、攻撃手法に関しては、ソフトウェアの脆弱性によってシステムを狙う手法と、フィッシング詐欺によって人間の心理を狙う手法を組み合わせた、より巧妙な攻撃が行われています。本来であれば、利用者は Web ブラウザのアドレスバー等を確認することで、フィッシング詐欺から身を守ることができますが、対象の Web サイトや利用中のソフトウェアに脆弱性がある場合には、画面をいくら注意深く確認しても、フィッシング詐欺の被害に遭ってしまいます。」と述べている。同書に掲載されている Web アプリケーションの脆弱性種別（2006 年）のグラフ（図 3.11）によると、クロスサイト・スクリプティングと SQL インジェクションが 2 大脆弱性となっている。

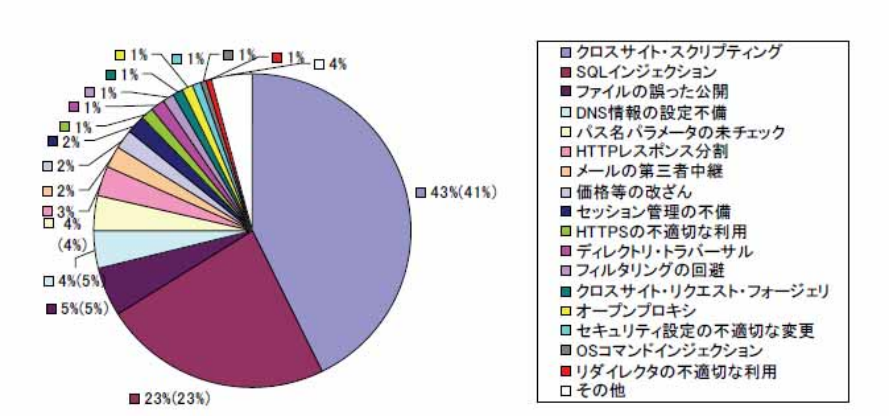


図 3.11 Web アプリケーションの脆弱性種別 (2006 年)

IPA（独立行政法人 情報処理推進機構）発行「情報セキュリティ白書 2007 年版」より

特に SQL インジェクション攻撃に関しては、IPA の 2008 年 5 月 15 日付 HP 掲載資料「SQL インジェクション攻撃に関する注意喚起」やセキュリティ検査会社である LAC 社の 2008 年 7 月 24 日付けレポートによると、2007 年～2008 年にかけ SQL インジェクション攻撃による Web サイトの改ざんや不正コードを仕掛けられたページ数が数十万に達している旨の情報がある。さらに「SQL インジェクションが突然増加した原因として SQL インジェクションを行うボット・ワームが出現したという情報もあります。攻撃者が多数のボットを踏み台にして、世界中に攻撃しているのではないかと推測しています。」（LAC 社レポートより）とのことで攻撃手法が進歩してきたことがわかる。

3.2. 本 WG の活動方針と調査方法

3.2.1. 活動方針

これまで述べたように EC を実現する Web サイトにまつわるセキュリティについては、様々な要因、関係者が関与している。さらに Web サイト構築や運営または Web セキュリティに関する資料、ガイドラインといったものもすでに世の中に沢山存在するなかで、本 SWG の活動方針を以下のように考えることとする。

まず、Web サイトセキュリティに関する全般的資料については、図 3.2.1 に示すように、IPA や有限責任中間法人 JPCERT コーディネーションセンター（JPCERT/CC）などの資料や、世界的には OWASP（Open Web Application Security Project）、WASC（Web Application Security Consortium）などの団体が発行している各種レポート、資料などですでに世の中に存在していると考えられるため、ここでは紹介程度に止める。

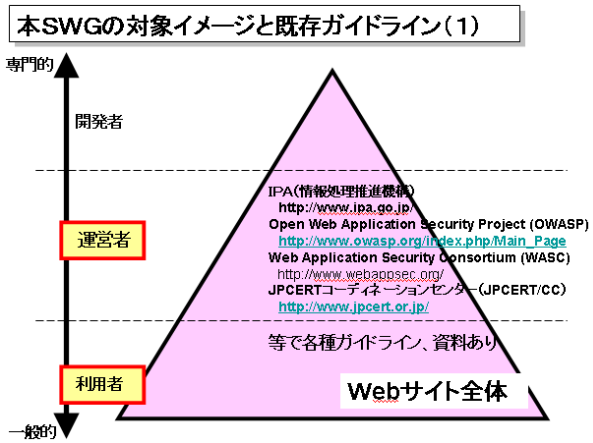


図 3.2.1 Web サイト全体の既存ガイド

次に、本 SWG で取扱うのは EC サイトであるので、図 3.2.2 に示すように一般的な Web セキュリティから EC に特化した部分を対象とする。

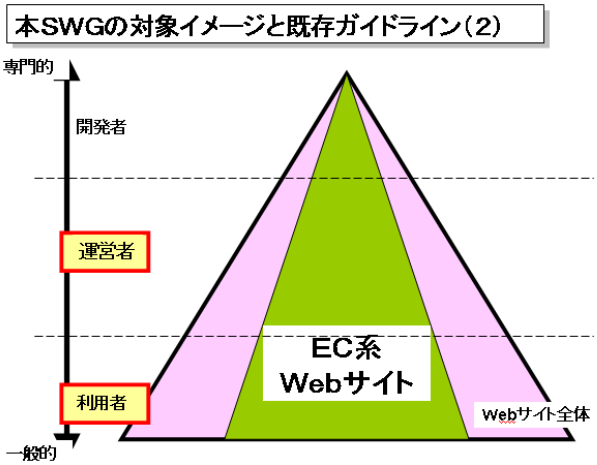


図 3.2.2 本 WG の対象 (1)

さらに前述したように EC サイト運営で特に注意しなければいけないことの 1 つに消費者の個人情報の取扱い、保護があげられるので個人情報保護の観点を入れ込み、大手ポータルに属さないような独立系の中小 EC サイトを意識しながらガイドラインにまとめていく。(図 3.2.3)

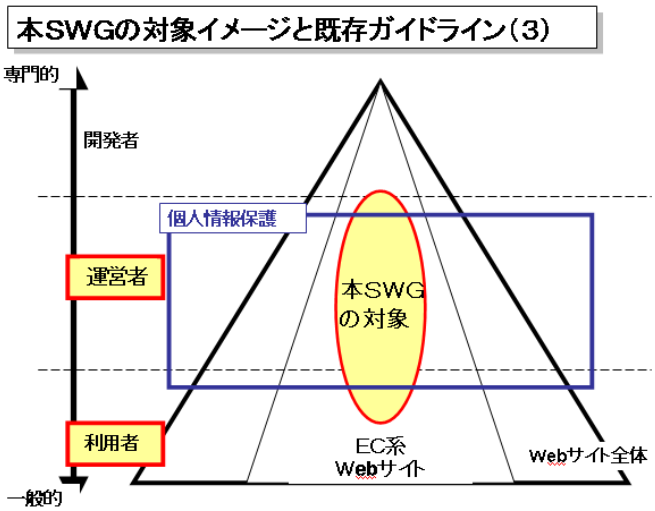


図 3.2.3 本 WG の対象 (2)

このようにまとめていくなかで、対象者を大きく Web サイト開発者、運営者、利用者に分類し、各々にとって役立つ内容がなにかを検討していく。

3.2.2. 調査方法

この検討の過程で、まず世の中の事例を収集する必要があるので、以下のような方法で主にインターネットを利用した事例調査活動を行った。

3.2.2.1 対象者分類

以下の分類で対象者を絞り、事例調査を行った。

①Web サイト開発・設計者　②Web サイト運営者（経営者）③サイト管理

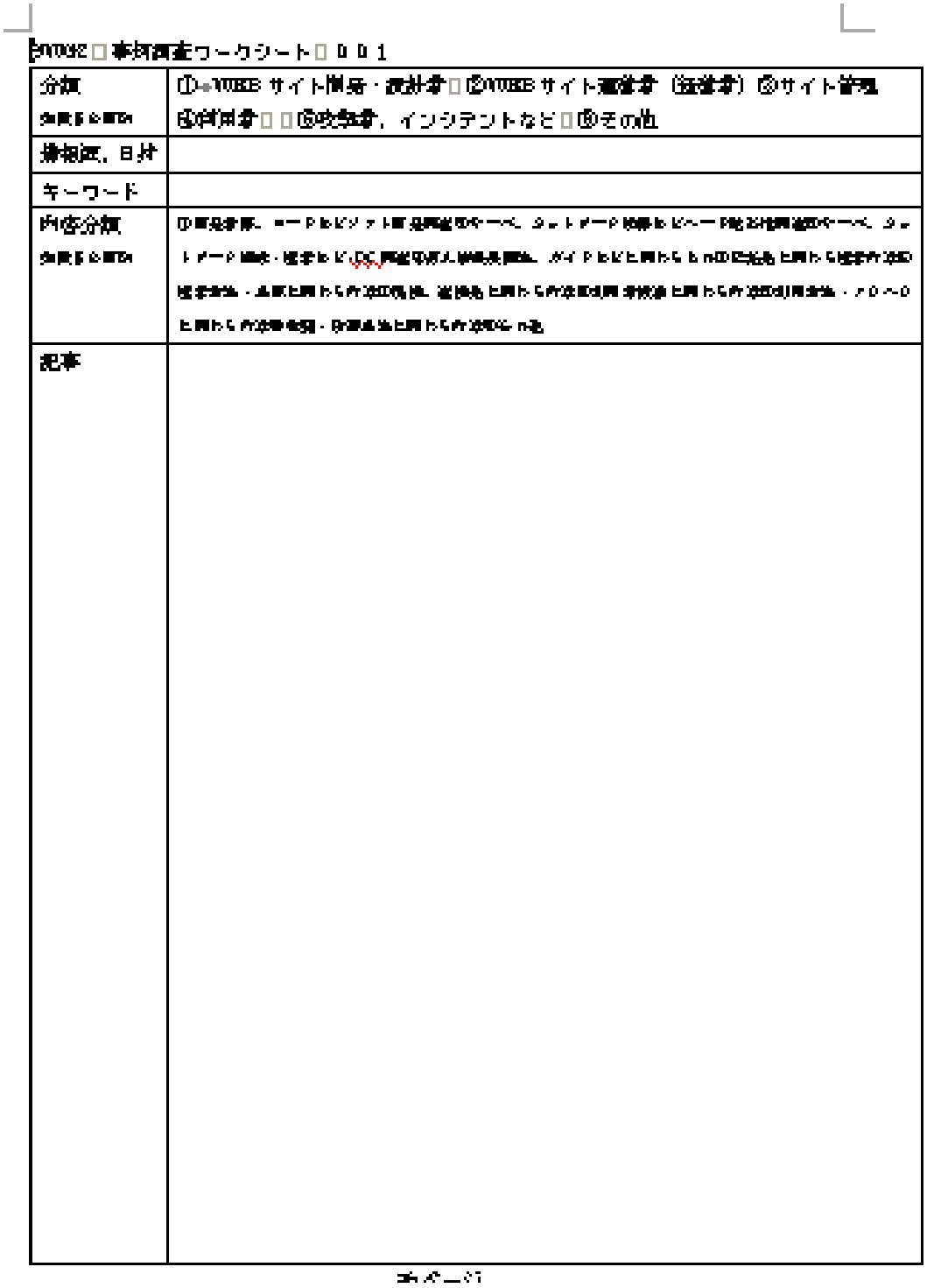
④利用者　　⑤攻撃者、インシデントなど　⑥その他

3.2.2.2 内容分類

さらに事例の内容を以下に分類する。

① 開発言語、コードなどソフト開発関連
② サーバー、ネットワーク機器などハード脆弱性関連
③ サーバー、ネットワーク構成・運営など iDC 関連
④ 個人情報保護法、ガイドなどに関わるもの
⑤ 委託先に関わる運営内容
⑥ 運営方法・手順に関わる内容
⑦ 提携、連携先に関わる内容
⑧ 利用者被害に関わる内容
⑨ 利用方法・ノウハウに関わる内容
⑩ 攻撃・防衛手法に関わる内容
⑪ その他

このように収集した事例を図 3.2.4 に示すワークシートにまとめた。



分類 （複数可）	①WEB サイト開発・設計者 ②WEB サイト運営者（管理者） ③サイト管理 ④利用者 ⑤攻撃者，インシデントなど ⑥その他
情報源，日付	
キーワード	
内容分類 （複数可）	① [illegible] ② [illegible] ③ [illegible] ④ [illegible] ⑤ [illegible] ⑥ [illegible] ⑦ [illegible] ⑧ [illegible] ⑨ [illegible] ⑩ [illegible] ⑪ [illegible] ⑫ [illegible] ⑬ [illegible] ⑭ [illegible] ⑮ [illegible] ⑯ [illegible] ⑰ [illegible] ⑱ [illegible] ⑲ [illegible] ⑳ [illegible]
記事	

図 3.2.4　事例収集ワークシート

3.2.3. 事例調査結果

このように調査した事例を各項目ごとに整理した表を表 3-1 に示す。

	①開発言語、コードなどソフト開発関連	②サーバー、ネットワーク機器などハード脆弱性関連	③サーバー、ネットワーク構成・運営などiDC関連	④個人情報保護法、ガイドなどに関わるもの	⑤委託先に関わる運営内容	⑥運営方法・手順に関わる内容
① Web サイト開発・設計者	8	0	3	0	0	2
②Web サイト運営者（経営者）	0	0	4	12	8	5
③サイト管理	0	0	18	0	0	9
④利用者	0	0	2	0	0	1
⑤攻撃者、インシデントなど	1	0	5	0	0	4
⑥その他	0	0	0	0	0	0
	9	0	32	12	8	21

	⑦提携、連携先に関わる内容	⑧利用者被害に関わる内容	⑨利用方法・ノウハウに関わる内容	⑩攻撃・防衛手法に関わる内容	⑪その他	計
① Web サイト開発・設計者	0	2	0	5	0	20
②Web サイト運営者（経営者）	3	3	1	4	1	41
③サイト管理	1	9	3	18	2	60
④利用者	0	21	22	7	3	56
⑤攻撃者、インシデントなど	0	7	6	40	0	63
⑥その他	0	0	0	0	0	0
計	4	42	32	74	6	240

表 3-1 事例調査表のまとめ

本事例調査では、延べ 155 に分類される計 120 の事例を収集できた。各事例の詳細については Appendix に添付した。

	事例数
① WEBサイト開発･設計者	13
②WEBサイト運営者（経営者）	27
③サイト管理	40
④利用者	33
⑤攻撃者、インシデントなど	42
計	155

表 3-2 各分類内訳

対象者ごとに特に関連する内容分類をあげると

① Web サイト開発・設計者に特に関連する分類
　1）開発言語、コードなどソフト開発関連
　2）サーバー、ネットワーク機器などハード脆弱性関連
②Web サイト運営者（経営者）に特に関連する分類
　4）個人情報保護法、ガイドなどに関わるもの
　5）委託先に関わる運営内容
　7）提携、連携先に関わる内容
③サイト管理に特に関連する分類
　3）サーバー、ネットワーク構成・運営など iDC 関連
　6）運営方法・手順に関わる内容
④利用者に特に関連する分類
　8）利用者被害に関わる内容
　9）利用方法・ノウハウに関わる内容
⑤攻撃者、インシデントに特に関連する分類
　10）攻撃・防衛手法に関わる内容

となる。
以降に各対象ごとに事例内容のあらましを述べる。

3.2.4. 各対象ごとの調査結果

一般に、Web サイトをたてるためには

1）コンテンツ系の検討

1. サイトコンテンツ検討（掲載内容、掲載ポリシーなど）
2. コンテンツ権利関係検討（コンテンツプロバイダー(CP)との著作権等権利処理）
3. コンテンツ調達検討
4. コンテンツ画面配置、ページ構成検討
5. コンテンツ運用検討
6. アプリケーション検討
7. 使用言語検討

2）サーバー機器検討

1. 機種検討
2. OS、ミドル検討
3. サーバー構成検討

3) データセンター検討

1. SLA など契約内容検討
2. ネットワーク構成、ラック配置、空調、電源検討
3. セキュリティ関係検討（F/W、IDS、IPS、WAF など）
4. 運用体制検討
5. 障害対応体制検討

4) 全体サービス検討

1. サービス運用ポリシー検討
2. CS 対応（問合せなど）検討
3. 開発、運用委託先検討
4. 入会契約、個人情報取扱いなど法務・情報セキュリティ系検討
5. その他

などの検討が必要であり、Web セキュリティに関してだけでも多面的に考慮する必要がある。今回は、第 1 回目の事例調査ということで Web セキュリティにまつわる概要がわかる程度にとどめている。特に Web サイト開発、設計者向けには、別途焦点を絞った調査が必要になると思われる。なお、サーバー、ネットワーク機器などハード脆弱性関連については対象なしなので対象からはずす。

3.2.4.1. Web サイト開発･設計者

Web サイト開発・設計者に関連する事例は計 13 事例を集めたが、Web セキュリティとハード機器との関連は元々薄いため今回は、収集事例はなかった。また、開発言語の PHP、JAVA スクリプトに関してのプログラム開発における注意事項などが数点収集できたが､実際に Web サイトを開発、設計する上で役立つ事例はあまり集められていない。
開発者、設計者向けには、焦点を絞ったさらなる調査が必要と思われる。

いずれにしても、開発者、設計者側で Web セキュリティ脆弱性に関する理解を深め、コーディングに際して注意を高める必要がある。PHP など注意が必要な言語を使用する場合などは、セキュリティを考慮されていないサンプルコードを安易にコピーして使用しないことはもちろん、各種開発ツールの導入などの工夫が必要である。

3.2.4.2. Web サイト運営者 (経営者)

Web サイト運営者むけの事例は 27 事例を収集した。特に個人情報を取り扱っているサイトに掲示されている各サイトの個人情報保護指針を中心に収集した。

どのサイトにも Web セキュリティに関連する項目としては、リンク先の他者の Web サイトに関わる問題や、クッキー（Cookie）に関する免責事項の記述がある。またクッキーを利用し、利用者のコンピュータからのアクセス状況を把握して､特定の Web ページの使用率等に関する統計を取ることができる技術である Web ビーコンについても使用範囲の記述がみられるサイトもある。

また委託先の事故、障害などの委託元責任に関わる事例も 8 例収集できた。個人情報漏洩など情報セキュリティ事故で委託先の監督責任を問われる可能性もあるので、委託先との契約内容、委託先セキュリティ基準の把握が重要になってくる。

万一、個人情報事故を起こした場合は、事故後の報道発表、被害者への説明、損害賠償などの処理を適切なタイミングで迅速に行わないと、信用問題や社会への影響がでる可能性がある。ケースに応じて監督官庁への報告も必要である。経営者は、このような事態に備えるべく、情報セキュリティ体制、事故対策マニュアルを常備し、必要に応じて対策本部設置などを実施すべきである。

3.2.4.3. サイト管理

Web サイトの管理にあたっては､Web サイトに必要なネットワーク回線速度､サーバー能力、多重化、障害時復旧時間などを的確に吟味して SLA（サービス・レベル・アグリーメント）を決定しておき、十分な投資対効果が得られるように委託を含む体制を確立することが重要である。情報セキュリティの観点では、守るべき情報（個人情報や秘情報）の有無、ある場合には格納場所を把握し､想定される脅威を事前に洗い出し対策を検討することが重要である｡このためには、脅威分析やリスクアセスメントと呼ばれる手法が有効である。また万一の事故に備え、被害総定額の算定が可能であれば、対策の投資額、範囲の決定がしやすくなる。

独立行政法人 情報処理推進機構が発行している「安全なウェブサイトの作り方 改訂第 3 版」の Web アプリケーションのセキュリティ実装の項では以下のインシデントが挙げられている。

1）SQLインジェクション

2）OSコマンド・インジェクション
3）パス名パラメータの未チェック／ディレクトリ・トラバーサル
4）セッション管理の不備
5）クロスサイト・スクリプティング
6）CSRF(クロスサイト・リクエスト・フォージェリ)
7）HTTP ヘッダ・インジェクション
8）メールの第三者中継
9）アクセス制御や認可制御の欠落

このうち、特に SQL インジェクションと、クロスサイト・スクリプティングが顕著な攻撃となっている。　今回の調査でサイト管理に関連するものでは 40 事例を収集した。実際にクロスサイト・スクリプティングや SQL インジェクションの攻撃にあい、個人情報漏洩事故を起こしたサイトの報告などが含まれている。

収集した事例によれば、2007 年～2008 年にかけ主に外国からの SQL インジェクション攻撃が急増しており、攻撃が営利目的化してきていることがわかる。企業秘密を売るのは労力がかかるが、個人情報は闇でも闇以外でもマーケットが確立しており流通経路に乗せやすいくリスクが少ないと考えられ、悪用した場合の価値が多いため後を絶たないと推測される。

サイト管理のうちサーバー側の管理としては、OS、ミドルなどのセキュリティパッチを常にウォッチして適切なパッチ修正をあてること、サーバーのディレクトリ、パス管理を適切に管理すること、アプリ等インストール時のデフォルト設定を適切に設定変更し脆弱性を残さないなどの管理が重要となる。

サーバー、ネットワーク機器の管理者権限、ID/PWD の管理の不備をつかれる事例も何例か収集されている。Admin、root などの管理者アカウントにはきっちととパスワードを設定することはもちろん、総当たり攻撃や辞書攻撃に耐える十分な長さの ID/PWD を設定することやパスワードを定期的に変更することが重要である。外部からの攻撃事例もあるが内部犯行のケースも多々あるので、管理者 ID/PW の定期的な棚卸し、チェックが必要である。特に退職者、担当変更などによる ID の削除は盲点になりやすい。退職者による内部犯行の事例も収集されている。

また、コンテンツアップ、サーバー・バージョンアップ、バッチあてなどの運用作業は、緊急事態、不測の事態を想定した運用マニュアルをきちんと用意し、メンバー交代などがあったとしても運用マニュアルがあれば問題なく作業実施できるようにするべきである。特に障害時、情報セキュリティ事故時のエスカーレーション先、事故後処理を事前にきちんと定めていないと、混乱を招くばかりか、二次災害や、事故当時の証拠保全ができなくなる恐れがあり、事後の捜査の妨げとなる。サイト管理では、このような人的内容を含む運用管理が重要な要素となる。

またサイト管理の技術的対策としては、ファイアウォール(F/W)の導入をはじめ、IDS（侵入検知システム）や IPS（侵入防御システム）を導してネットワークセキュリティ対策を施すことが効果的である。最近では UTM（Unified Threat Management：統合脅威管理）の導入が主流となると考えられている。UTM 製品は、複数の機能の設定や管理を統合し、様々な種の脅威動向を管理･防御できるため、管理に要する手間やコストを大幅に削減できるというメリットがある。

さらに、本来管理権限の無いドメインの情報をいろんな DNS サーバーに勝手に送りつけて、

そのドメインを乗っ取ってしまう攻撃である DNS キャッシュ・ポイズニングや DNS 脆弱性問題などが問題視され、サーバーだけでなく DNS 管理も重要な項目となる。

しかしながら、Web アプリのセキュリティ対策という観点では、IDS、IPS だけでは不足で、SQL インジェクションのように、80 番ポートに対する正規の HTTP リクエストでやってくる攻撃に対しては Web アプリケーションのパケットフローを検査する Web アプリケーションファイアウォール（WAF）の設置のほか、Web アプリケーション開発のライフサイクルに、セキュアなアプリケーションにするための仕組みを導入することなどが考えられる。また最近では Data Loss Prevention（DLP）を導入し、クライアントとゲートウェイ間で情報漏えい対策を施すツールも提供されている。いずれのツールも実際の使いこなしにはかなりの運用ノウハウがいるためベンダー含めた事前検討を十分にする必要がある。また信用できる運用会社に委託し遠隔監視サービスなどを利用することも可能である。

PDCA をまわす開発ライフサイクルのなかで、Web アプリケーションの脆弱性検査を実施することは現実的な効果がある。収集した事例では、HP WebInspect、IBM Rational AppScan といった検査ツールを利用した定期的な検査を実施することにより、静的な問題だけでなく、実際の Web サイトの動的動作を含めたトータルな検査が可能となる。

セキュリティ検査会社では、SOC（Security　Operational　Center）を運営しているところもあり、SOC に定期的な検査、侵入検知を依頼する方法もある。Web セキュリティ検査ツールは、あらかじめ用意された攻撃パターンにそって自動的に擬似攻撃をかけるオート機能がついたものがほとんどであるが、実際の検査にあたっては、ページ遷移やＤＢ構成などを考慮したマニュアル操作の検査が主体となる。特に重要な Web サイトについては、上記 SOC などの熟練メンバーを交えた検査体制、スケジュールを組む必要がある。

また、実際に個人情報事故にあった Web サイト管理者の事例として、リンクされなくなった古いファイルは検査の対象外となってしまい消し忘れていたページの脆弱性を突かれたり、検査時点で脆弱性のあるページを見逃した可能性も指摘されている。

さらに一般的にはこのような検査は、Web サイトに対して擬似攻撃を仕掛けるため、本番サイトでは影響が甚大なため、テスト用のサイトに移して検査を実施する。このため、実は本番サイトの環境を忠実に反映していない場合もあるので注意が必要である。

サイト管理については、

1）データセンターでのサーバー運用、各種ツール導入

2）コンテンツアップなどコンテンツ運用

3）セキュリティ検査、ツール

の観点でさらなる調査を実施すれば効果的だと思われる。

3.2.4.4. 利用者

利用者に関する事例は 33 事例収集した。

内容的には、利用者が被害にあった事例、被害にあわないようにする利用ノウハウ、利用者を狙った攻撃手法などに分類された。

利用者が被害にあった事例のなかでは、主に銀行、金融機関を狙ったフィッシング詐欺の被害事例が多かった。被害にあった銀行の Web サイトに掲載された被害状況、利用者への注意事項な

ども事例として収集した。

フィッシングの手口としては、銀行を騙って「重要なお知らせ」といった件名で、実際の銀行のサイトとは異なる URL へのアクセスを促し、ログインパスワードやインターネット用暗証番号などを盗もうとする手口がほとんどで、フィッシング対策協議会（http://www.antiphishing.jp/）によると毎月数件～数十件の被害が報告されている。

フィッシング対策協議会、警察、銀行、法テラスなどの HP でフィッシング詐欺に対する注意喚起がなされている。注意喚起の内容としては

1）**個人の金融情報（クレジットカード番号、ID、パスワード等）を聞き出そうとする不自然なメールに対しては、メールを送信してきたとされる企業の実際のホームページや窓口に問い合わせて確認する。**
2）**ブラウザの URL を確認し、正規の銀行サイトであることを確認する。**
3）**個人情報入力ページでは、通常 SSL 通信になっているので、ブラウザに SSL 通信を示す「鍵のマーク」がロックされた状態で表示されているか確認すること。さらに「鍵のマーク」をクリックしてホームページが正規の企業のものか確認することを習慣づける。**
4）**アクセス先が固定の銀行、金融機関の場合は、アクセス先の URL をブラウザの**ブックマーク機能を利用して、ブックマーク登録する。
5）**銀行によっては、**EV SSL 証明書の導入をしているところがあるので、EV SSL 証明書対応のブラウザにてアドレスバーが緑色に変わり、アクセスしたサイトが正規サイトであることを確認する。

などを挙げている。

また、**都道府県警察のサイバー犯罪相談窓口では、フィッシング 110 番を開設し、フィッシングに関する情報提供を受け付けている。**

最近では、セキュリティ関連会社、ブラウザ提供組織などが、不正サイト、要注意サイトのブラックリストを用意しており、端末側ブラウザのプラグインなどを利用してインストールしたり、プロキシサーバーでフィルタリングしたりすることが可能となっている。
EV SSL 証明書の利用も今後進むと考えられる。

利用者側での注意事項としては、セキュリティに考慮したブラウザを利用することや、ブラウザのセキュリティ設定を用途に合わせて適切に設定することがあげられる。
また、ブラウザの脆弱性、セキュリティホールなどは最新パッチ情報にあわせて、日ごろから最新版にアップグレードしておくことも大事である。マイクロソフト社が提供するインターネットエクスプローラ（現状最新版 IE7）以外にも、オープンソース系の Firefox、Opera などのブラウザなど多数あるので用途によりブラウザを使い分けてもよい。

ブラウザの設定では、クッキー受入条件、ポップアップ画面表示条件、Javascript 動作条件、証明書受入条件などを設定可能であることが多い。

携帯電話に対しては、出会い系に関連する事件、オレオレ詐欺など相次ぐ事件の急増を契機に、総務省等の検討会、青少年ネット規制法の議員立法活動により、未成年に対するフィルタリング

サービスの義務化、携帯電話、PHS 事業者へのカスタマイズ機能実装要請、健全なサイトの基準策定、認定を行う民間第三者機関設置などの動きがある。

これらの動きは現状の現場実情を必ずしも反映していない面もあり、技術的な現実的解決策が追いつけないケースがでたり、ホワイトリスト方式で利用者自身のサイトをみることができないケースなど無害のサイトまで規制したりする混乱も一部みられるが、ある程度の知識を保有する利用者を想定できるパソコンとは異なり、携帯電話では高齢者、未成年などが手軽に利用できるため必要な動きと考えざるをえない。端末開発業者、サービス業者、キャリア、ISP 業者など関係者の協力で適切な運用体制になっていくことを願う。

3.1.で述べたように、EC サービスはパソコン、携帯のみならず、TV 他の情報家電にも発展していっているので、今後各方面で協力した検討活動が必要になると思われる。

3.2.4.5 攻撃者、インシデントなど

合計 42 の事例を収集できた。

IPA 他、セキュリティ検査会社が発表している報告書をみても、近年 Web セキュリティ事故につながる攻撃が急増していることがわかる。特に、海外での攻撃が顕著であり、世界的には米国、中国、欧州などで様々なインシデントが急増している。世界レベルでみると日本はまだ比較的インシデント数が少ないといえるが、特に昨年あたりから海外からの攻撃が顕著となっており、フィッシング、SQL インジェクション、クロスサイト・スクリプティングなど特定の攻撃がある時期に集中する傾向がある。

ボットネットによる攻撃も急増しており、攻撃元を特定できないことも注意すべきことである。

事例にもあるように、特に海外ではブラックマーケットが組織的に運営されているようで、個人情報を保有するサイトは攻撃対象になると考えたほうがよい。最近の傾向では、特に SQL インジェクション攻撃が盛んであり、クロスサイト・スクリプティングとともに特に注意すべき攻撃でありう、定期的な検査が推奨される。また、サイト管理の項でも述べたようにこれ以外にも攻撃手法はあるので、総合的な検査実施が望まれる。

外部からの攻撃に対しては、守るべき情報がなにかをきちんと把握したうえで、脅威分析などの手法を利用して事前に脅威を想定し、適切なサーバー、ネットワーク構成の構築、侵入に対する監視体制の確立、アクセスログの定期的なチェックを実施し不正侵入の有無を早期にチェックすることが重要である。

また、統計的には内部犯行のケースも多数あるため、ある程度性悪説にたった管理体制を敷くのもやむを得ない。特に退職者、担当変更、委託先変更などによる管理者 ID の廃棄、変更管理は見過ごされやすく、万一悪意の犯行が会った場合には、容易に重要情報にアクセスできるため非常に重要な対策となる。

攻撃は被害があるばかりでなく、サーバー乗っ取りや踏み台にされるなどで無関係の第三者に対して加害者になってしまう可能性もある。この場合、法的対応など微妙で対応困難なケースが多く、対策本部設置、関係各所への連絡など迅速かつ適切な対応が要求される。

今回、インターネット上での公開情報による事例収集という手法を用いたため、多数の事例は集まったが、当然公開情報のみのため、被害状況、インシデント・レスポンス状況、再発防止対策内容など被害をうけた当事者にとって重要な情報は入手不可能である。

本来はこのような事例をまとめるべきであろうが､公開を前提とした調査では限界があるため、国内では IPA、JP/CERT などの機関などがあるので個別の対応に期待する他はない。セキュリティ会社の公開脅威情報、セキュリティレポートなどに定期的に入手し、インシデント傾向を把握することは重要である。

また、被害にあってからの対策、原因究明、関係部署への連絡、再発防止案検討のためにインシデント・レスポンス・チーム（IRT）を組織することも検討すべきである。このような支援サービスを提供するセキュリティ会社もある。

3.3. まとめ

今回、Web セキュリティ SWG として、近年問題視されている Web セキュリティにまつわる課題の抽出とガイドライン策定を目的として活動を行った。

方針で述べたように、本活動の対象者を、Web サイトの開発者、運営者、利用者に分類し、事例調査を行った。調査は主にインターネット上の調査にとどめ、インターネット上で一般公開されている範囲にとどめた。なお、収集事例では、公的機関、公的機関代表者などを除き、被害者、加害者および宣伝目的で個人または団体を特定できるものは伏せ字にしてある。

今回、120 事例（分類にして延べ 155 種類）の事例を収集できた。SWG のメンバーの方々のご協力に感謝いたします。

今回分類としては以下をもうけた。

①Web サイト開発・設計者　②Web サイト運営者（経営者）③サイト管理

④利用者　　⑤攻撃者、インシデントなど　⑥その他

キーワード検索、関連企業、HP などを調査したが、収集事例で、インシデント関連の事例が多数収集できたことはある意味意外であり、特に最近になっていかに Web セキュリティ被害が増加しているかを実感させるものであった。

Web セキュリティ全般では IPA、JP/CIRT などの HP で、すでにガイドライン、参考資料が掲載されているのでそちらを参照されたい。利用者の保護という観点では、総務省、経済産業省、他監督官庁の HP、警察、消費者センター、法テラスなどに、ガイドライン、注意喚起などが掲載されている。巻末に今回の報告で参考とさせていただいたサイトをまとめた。

今回の調査は第 1 回調査であり、全体を把握するいわば予備調査のような位置づけであると認識している。各項目でも述べたが、ガイドライン策定への次ステップとしては、各対象ごとに目的を絞って、さらなる追加調査が必要である。

参考文献

1）経済産業省　「平成 18 年度電子商取引に関する市場調査」

2）公正取引委員会　「平成 18 年度電子商店街等の消費者向け e コマースにおける
取引実態に関する調査報告書」

3）IPA（独立行政法人　情報処理推進機構）　「情報セキュリティ白書 2007 年版」

4）IPA（独立行政法人　情報処理推進機構「安全なウェブサイトの作り方 改訂第 3 版」

5）LAC 社　JSOC　「SQL インジェクション緊急レポート」2006 年 3 月

6）シマンテック社　グローバルインターネットセキュリティ脅威レポート　2007 年 7 月

7）ウェブサイト運営者のための脆弱性対応ガイド　2008 年 4 月
独立行政法人 情報処理推進機構
有限責任中間法人 JPCERT コーディネーションセンター
社団法人 電子情報技術産業協会
社団法人 コンピュータソフトウェア協会
社団法人 情報サービス産業協会
特定非営利活動法人 日本ネットワークセキュリティ協会

8）ネットワークセキュリティ Expert1-8　　技術評論社

関連するサイト一覧（順不同）

□ 政府系サイト

独立行政法人 情報処理推進機構　セキュリティ関連

http://www.ipa.go.jp/security/index.html

内閣官房情報セキュリティセンター

http://www.nisc.go.jp/

METI 経済産業省　情報セキュリティ政策室（商務情報政策局）

http://www.meti.go.jp/policy/netsecurity/index.html

MIC 総務省：　情報セキュリティ対策室（情報通信政策局）：

http://www.soumu.go.jp/joho_tsusin/security/mail.htm

MIC 総務省　政府認証基盤(GPKI)（行政管理局）

http://www.gpki.go.jp/

NiCT 独立行政法人　情報通信セキュリティ研究センター：

http://www2.nict.go.jp/y/y201/src-web/

JIPDEC （財）日本情報処理開発協会

http://www.jipdec.or.jp/

情報セキュリティ対策室

http://www.jipdec.or.jp/security/security.html

電子商取引推進センター

http://www.ecom.jp/ecpc/index.html

サイバークリーンセンター

https://www.ccc.go.jp/

□ 利用者保護関連サイト

法テラス

http://www.houterasu.or.jp/

国民生活センター

http://www.kokusen.go.jp/map/

NPA 警察庁： サイバー犯罪対策：**http://www.npa.go.jp/cyber/**

@police：http://www.cyberpolice.go.jp/

フィッシング対策協議会

http://www.antiphishing.jp/

□ 本報告書で参考とした各セキュリティ会社 公開情報など

シマンテック社 セキュリティレスポンス ホワイトペーパー
http://www.symantec.com/ja/jp/business/security_response/whitepapers.jsp

LAC 社 JSOC 侵入傾向分析レポート
http://www.lac.co.jp/info/jsoc_report/

マカフィー社 セキュリティ解析センター
http://www.mcafee.com/japan/security/

NTT コミュニケーションズ社 法人総合
http://www.ntt.com/business/

トレンドマイクロ社 最新ウイルス事情
http://jp.trendmicro.com/jp/products/personal/vb2008/latest_virus_information/index.html

日本エフ・セキュア株式会社
http://www.f-secure.co.jp/

Web セキュリティ SWG（SWG2） メンバーリスト

（敬称略）

参加区分	氏名	会社名
会員メンバー	保倉　豊	グローバルフレンドシップ株式会社
	川城　三治	グローバルフレンドシップ株式会社
	森岡　竜司	株式会社小松製作所
	高瀬　秀一	電気事業連合会
	平野　芳行	日本電気株式会社
SWG リーダ	岩本　幸治	パナソニック株式会社
	吉竹　弘幸	みずほ情報総研株式会社
	松浦　陽亮	三菱電機情報ネットワーク株式会社
有識者	辻　　秀一	東海大学
	荒川　一彦	近畿大学
	成瀬　一明	株式会社　東芝
	岩田　修	オフィス　イワタ
	高橋　和博	株式会社テプコシステムズ
	垣内　伯之	日本情報処理開発協会
オブザーバー	清水　友晴	経済産業省 情報セキュリティ政策室
	和田　浩明	経済産業省 情報セキュリティ政策室
主査	再起　和夫	パナソニック株式会社
事務局	合原　英次郎	次世代電子商取引推進協議会
	川嶋　一宏	次世代電子商取引推進協議会

4. PKI 適正運用･利活用 SWG 活動報告

4.1. 活動概要

（1） 目的

近年、ネットバンキングやオークション等に代表される ICT 上の商取引が個人のレベルに急激に普及している。そのような中で盗聴、改ざん、なりすまし、事実否認等の電子商取引におけるリスク回避に有効なインフラとして、PKI（Public Key Infrastructure：公開鍵暗号方式)が幅広く活用されている。この PKI については、当初、正しい理解に基づく運用・利用になかなか結びつかなかったという側面がある。2005 年頃には正規の運用者によるオレオレ証明書、セキュリティ無視の利用手引き等が横行していた。今日においては、殆どの大手金融関係やメジャーなサイトでは正しい運用がなされているものの、まだまだ誤った運用がなされているケースが存在すると思われる。また、仕組みの複雑さから、利用者サイドの理解が進まず、安全確認での利用が促進されないといった現状がある。このような中で、ICT での電子商取引が、物品/コンテンツ販売・オークション等の小額個人取引を中心に拡大し、経済犯罪（ID 等の詐取、金銭詐欺）の危険性が増加し、セキュアな通信・決済へのニーズはますます高まってくるものと思われる。また、ICT 上の商取引への新規参入企業が増加することから、2005 年頃の状況が再発し、オレオレ証明書の犯罪利用や不正確な運用をついた経済犯罪の発生が予想される。このような背景から本 SWG では、PKI の適正運用・利活用に資する目的で、PKI 活用の代表事例である SSL の運用実態の調査・分析を行うこととした。

（2）活動経過

活動経過は表 4-1 の通りである。

表 4-1 情報セキュリティリスク研究 SWG の活動経過

期日	活動内容
平成 20 年 6 月 13 日	第 1 回情報セキュリティ WG
7 月 31 日	第 1 回 PKI 適正運用・利活用 SWG
	・IPA セキュリティセンター情報セキュリティ分析ラボラトリー 小松ラボ長による講演を実施 ・PKI の誤った使い方の事例調査（～9 月 22 日）
9 月 24 日	第 2 回 PKI 適正運用・利活用 SWG
	・事例調査の集計結果報告 ・報告書目次案の検討
9 月 29 日	第 2 回情報セキュリティ WG
11 月 18 日	第 3 回 PKI 適正運用・利活用 SWG
	・報告内容（纏め方）について
11 月 26 日	第 3 回情報セキュリティ WG
	・今年度報告内容レビュー
平成 21 年 2 月 6 日	第 4 回情報セキュリティ WG
	・活動成果報告書確認

4.2. 事例調査

4.2.1. 事例調査の方法

ECOM 会員のホームページ（1 社あたり 1 ページ）及び、SWG メンバーで日頃使っているホームページ等を中心に、個人情報等の入力がある ECOM 会員及び任意のホームページを対象に調査を行った。

4.2.2. 調査結果

今回の調査では、調査対象の総数を確認しなかったため、調査対象全体に占める問題のあるサイトの割合については不明であるが、問題のあるサイトが相当数発見された。これらのサイトには著名なものも多く含まれており、サイトの信頼性確保について、まだまだ認識が足らない事をうかがわせる結果となった。

以下に、調査結果を示す。

表 4-2 個人情報等の入力について問題がある HP（ECOM 会員企業以外）

個人情報等の入力について問題があるHP（ECOM会員企業以外　2008.09.24現在）									
業種(確認サイト数)	httpからhttpsへの通信	個人情報やユーザID/PW入力HPにSSLを使っていない	主画面と入力画面のドメイン名が異なる	証明書の記載とドメイン名が異なる	Verisign Secured Sealの不適切な使用	右クリックが禁止されている	アドレスバーが表示されない	証明書の期限切れ	自分自身で発行した証明書を使っている
IT関連(6)	1	1	1	2	1			2	
交通・宿泊予約等(3)	3								
教育関連(1)		1			1				
金融・保険関連(10)	1		3	4		4	1		
ネットSHOP(3)		1	2				1		
官公庁・法人等(3)		2							1
情報提供(1)	1								
医療(1)								1	
合計（28）	6	5	6	6	2	4	2	3	1

表 4-3 個人情報等の入力について問題がある HP（ECOM 会員企業）

個人情報等の入力について問題があるHP（ECOM会員企業　2008.09.24現在）			
業種（確認サイト数）	httpからhttpsへの通信	個人情報やユーザID/PW入力HPにSSLを使っていない	主画面と入力画面のドメイン名が異なる
IT関連(3)	1	2	1
金融・保険関連(1)	1		
官公庁・法人等(4)		4	
合計(8)	2	6	1
＊複数HPを有する会員もあるが、1会員あたり1HPを調査対象とした			

今回の調査では、サイト内で異なるドメイン名を利用している事例や、証明書の記載に誤りや期限切れ等がある事例、http で書かれたページへの入力内容を hppts へポスト(送信)している事

例等が多く発見された。これらの問題点について事項で説明を行なう。

4.2.3. 事例の解説

以下、今回の調査で明らかになった問題のあるサイトの事例を解説する。

（1）http で利用者へ送信されたホームページから https サーバーへの通信

何らかの事情で個人情報等の保護すべき情報を入力する画面（以下、入力画面）が http によって送信されており、当該入力画面から入力されたデータの送信のみを https で行っている事例。本事例は一見安全にみえるが、http では通信内容が保護されないため、利用者 PC へ送信された入力画面そのものが通信経路途上で改竄されている可能性がある。

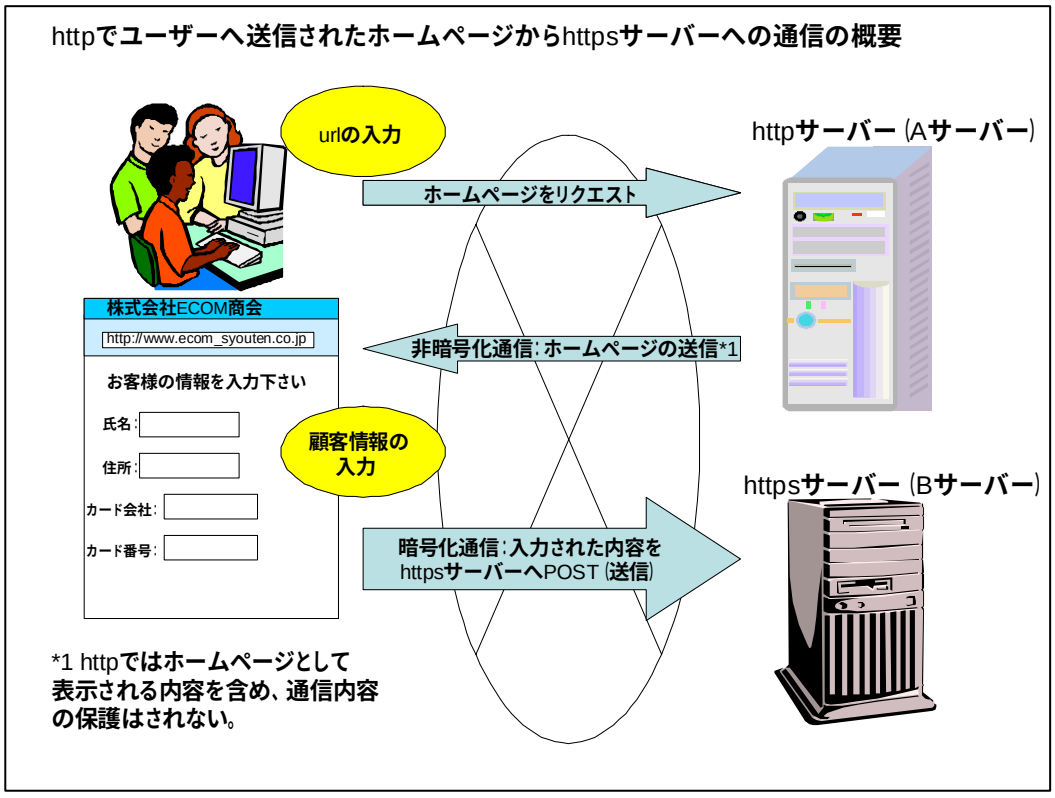


図 4.2-1 http でユーザーへ送信されたホームページから https サーバーへの通信の概要

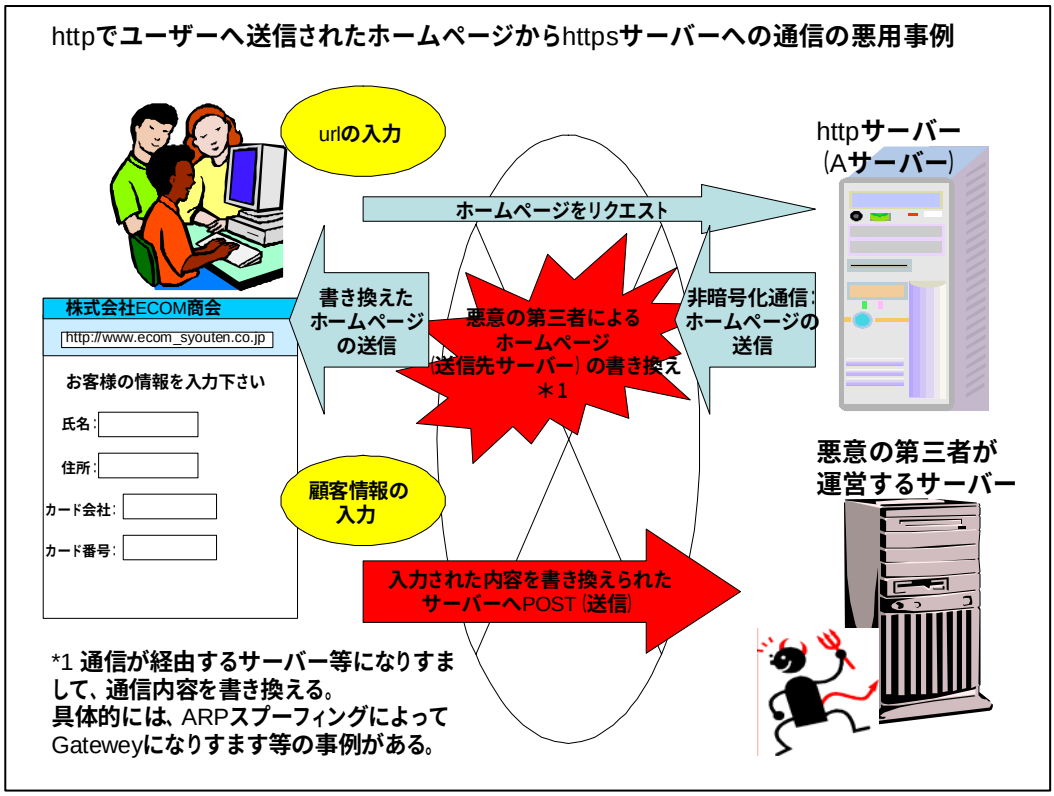


図 4.2-2　http でユーザーへ送信されたホームページから https サーバーへの通信の悪用事例

（2）重要な情報の入力ホームページに SSL を使っていない

本事例は、個人情報やユーザーID/パスワードといった重要な情報を入力する画面に SSL と適用していないというものである。（1）でも述べたが、http では通信内容は一切保護されない。このため、個人情報やユーザーID/パスワードといった重要な情報を入力する画面には https を適用することが望ましい。

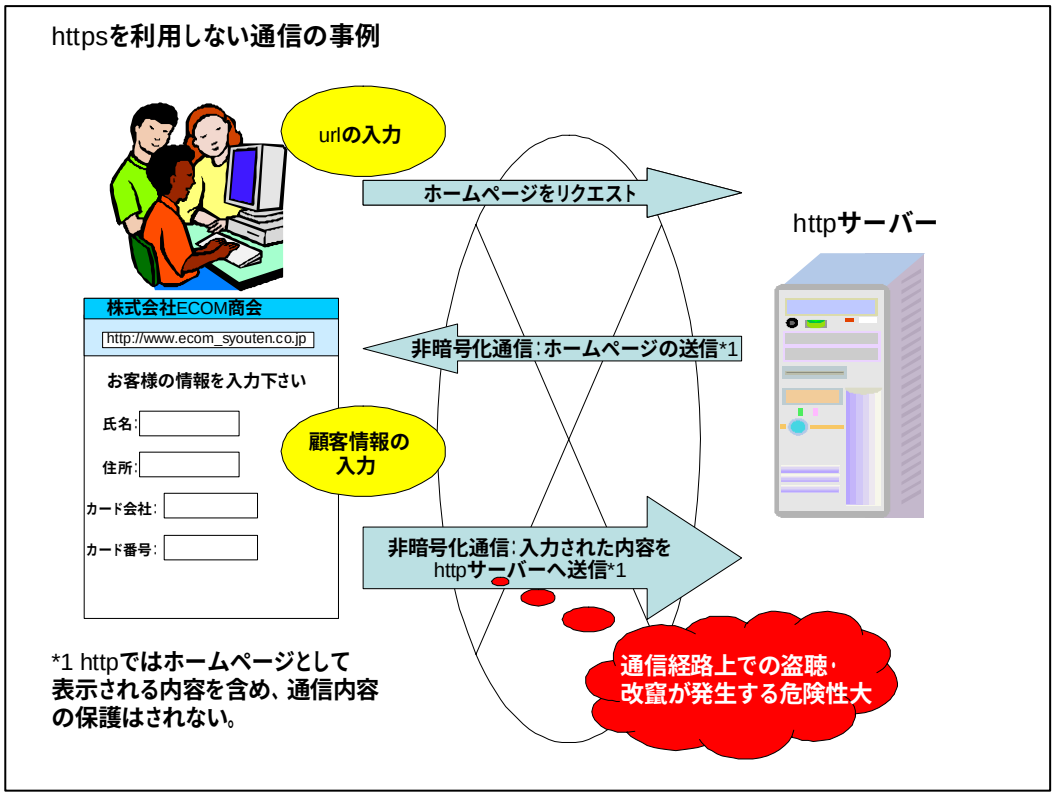


図 4.2-3　https を利用しない通信の事例

（3）サービス提供者と入力画面のドメイン名が異なる

本事例は、サービス提供者のドメインと個人情報やユーザーID/パスワードといった重要な情報を入力する画面のドメインが異なるというものである。利用者からの情報入力の委託等を行っている場合に多く見受けられる。ドメイン名が異なる場合、利用者は入力画面がサービス提供者のものかどうか確認が困難である。また、利用者が情報の入力時に証明書を確認しても、入力画面の正当性を確認できるものの、正しい相手に対するものであるかどうかの確認はできない。またフィッシング詐欺等においても、利用者を気づかない間に異なるドメインへ誘導し、重要な情報を入力させるケースがあることから、本事例はフィッシング詐欺と見分けがつくにくく、好ましくない運用事例であるといえる。

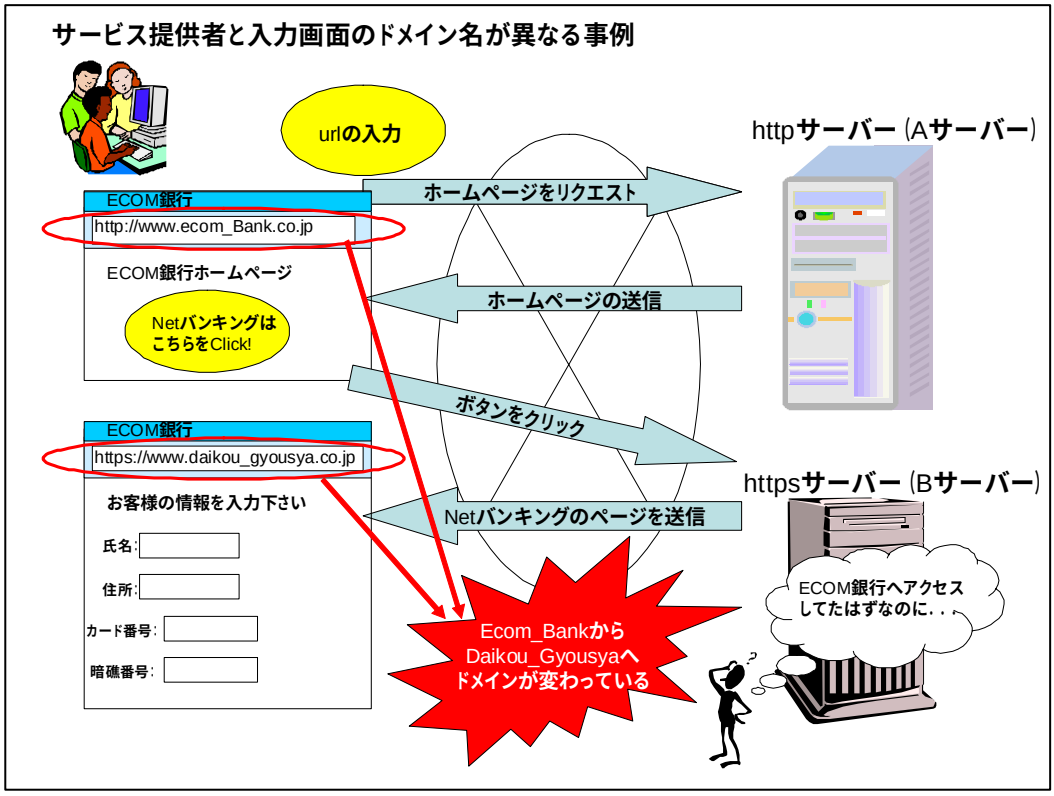


図 4.2-4　サービス提供者と入力画面のドメイン名が異なる事例

（4）証明書の記載とドメイン名が異なる

本事例は、サービス提供者のドメイン名と証明書に記載されるドメイン名が異なるというものである。原因としては、証明書入手後にドメイン名の変更を行った場合等が考えられる。いずれにせよ、証明書のドメイン名と現行のドメイン名が異なれば、何らの正当性の証拠にならない。本事例も前出のサービス提供者と入力画面のドメインが異なる事例と同じく、フィッシング詐欺と見分けがつきにくく、好ましくない運用事例であるといえる。

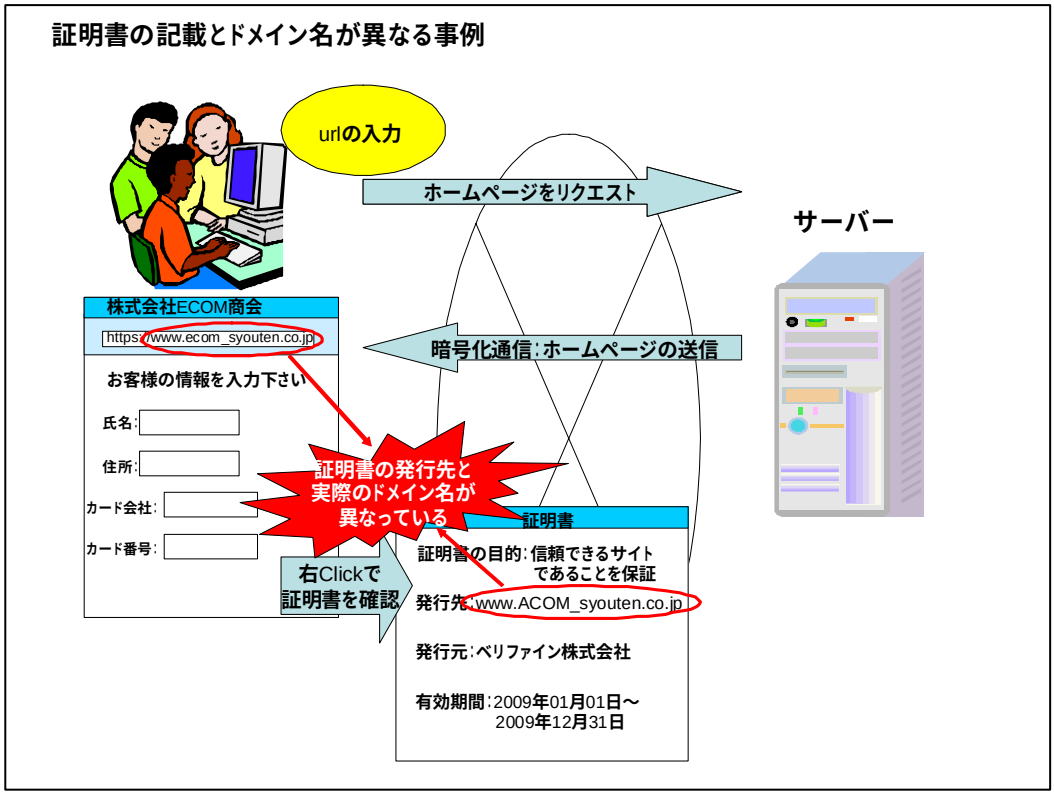


図 4.2-5　証明書の記載とドメイン名が異なる事例

（5）Verisign Secured Seal の不適切な使用

Verisign Secured Seal は、証明書の発行機関である Verisign 社が発行するマークである。本マークは、本マークを表示しているホームページが SSL 暗号通信を使用した安全なサイトであることを表す。通常、ホームページ上に表示された当該マークをクリックすると、当該ホームページの持ち主である企業や組織の名称、Verisign 社による SSL の検証状況、サイト名等が掲載される Verisign 社のホームページが表示される。本事例は、この Verisign Secured Seal をビットマップのみとして表示しているというものであり、Verisign 社による検証を受けたサイトであるかどうかが確認できない不適切な運用事例である。

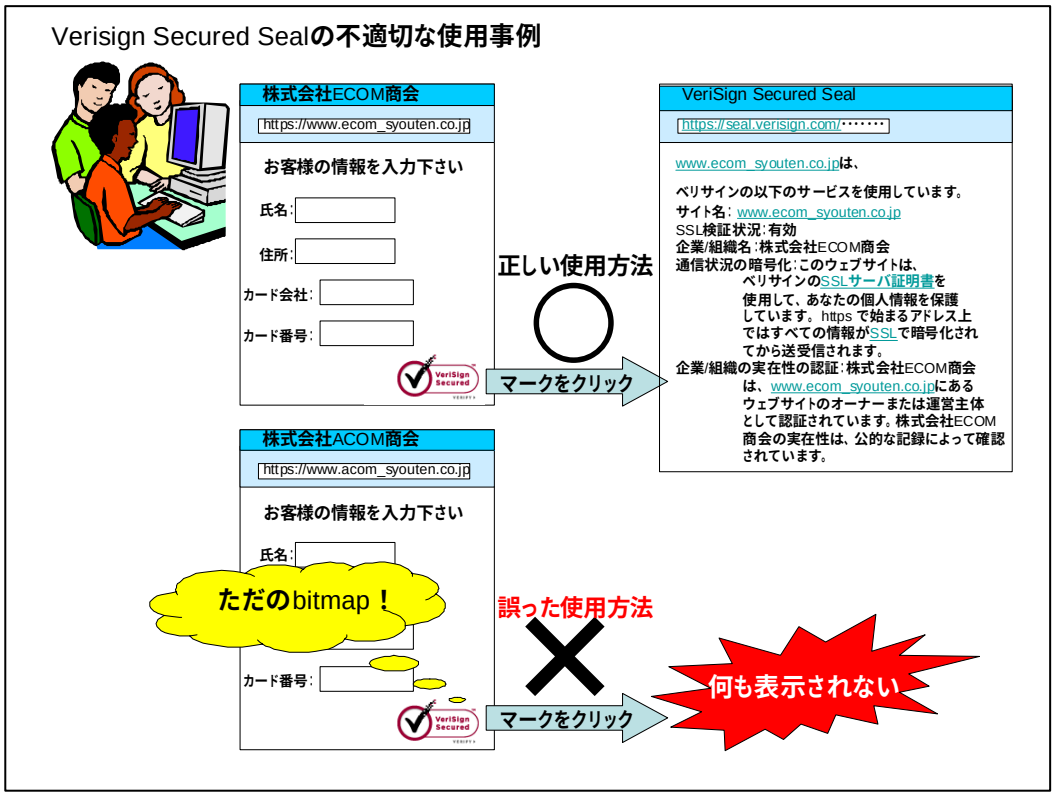


図 4.2-6　Verisign Secured Seal の不適切な使用の事例

（6）右クリックが禁止されている

本事例は、右クリックが禁止されており、利用者は右クリックによる証明書の確認が行えないというものである。予期せぬプルダウンメニューの表示等に対する利用者からの問合せ対策として、意図的に右クリックを禁止する等の場合が考えられるが、セキュリティ上は問題となる。本来、ホームページ上の任意の場所を右クリックすると、プルダウンメニューが現れ、そこからプロパティを選択することにより証明書の内容を確認できる。

＊ブラウザの表示オプションでステータスバーの表示を選択している場合、ステータスバー（ブラウザ最下段に表示）右側の鍵マークをクリックすることでも証明書は確認できる。

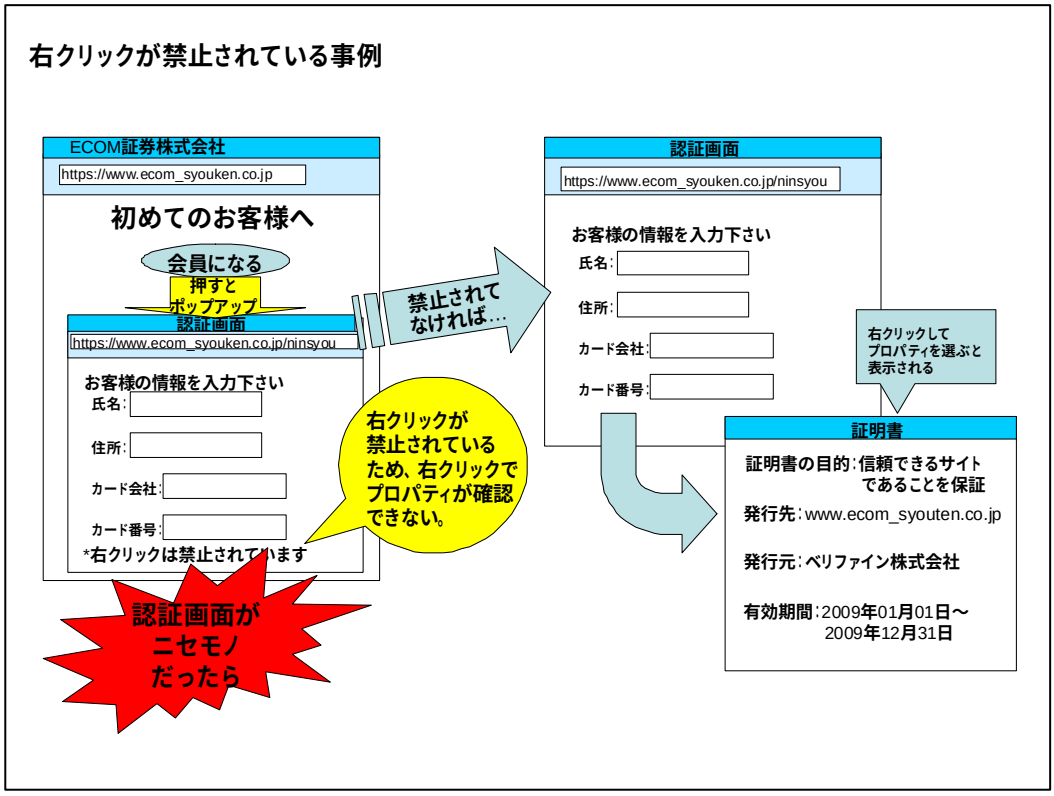


図 4.2-7　右クリックが禁止されている事例

（7）アドレスバーが表示されない

本事例は、SSL の運用実態とは直接関係ないものの、セキュリティ上の不備という観点で本報告に記載する事とした。本来、ブラウザにはアドレスバーが表示されており、アクセス中のホームページのアドレスが確認できる。本事例では、アドレスバーが表示されないため、アクセス中のホームページのアドレス確認ができない。ボタン等をクリックすることによって表示されるポップアップウィンドウ等の場合に多い。

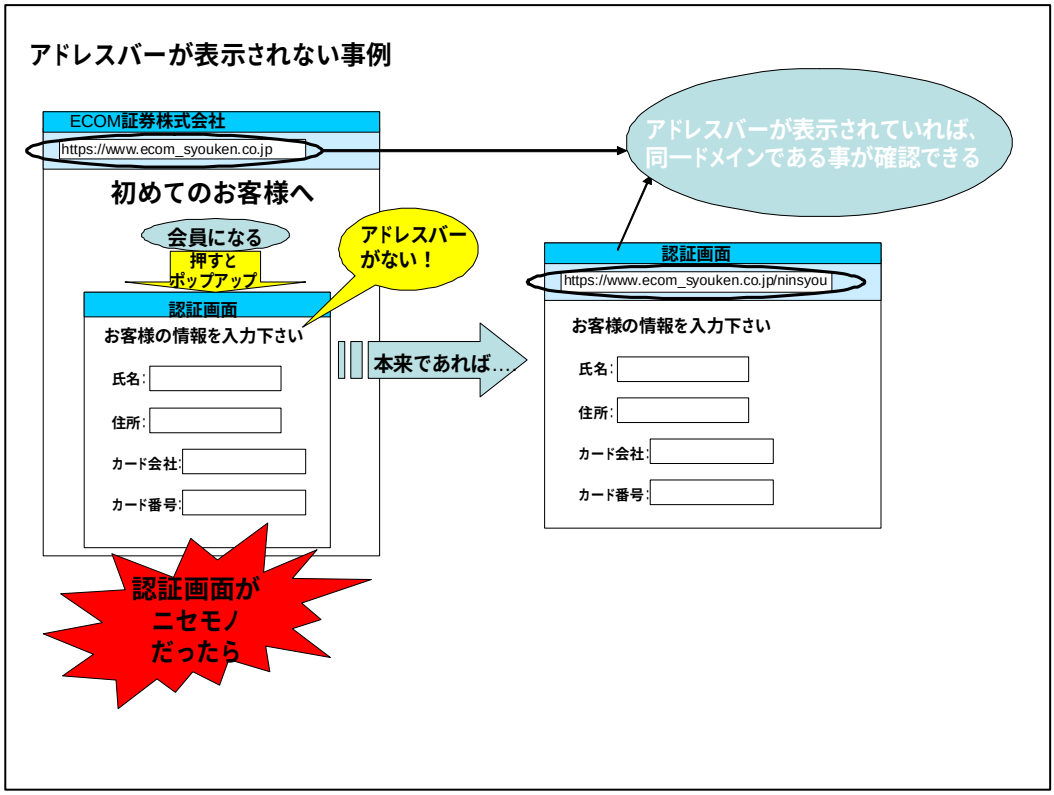
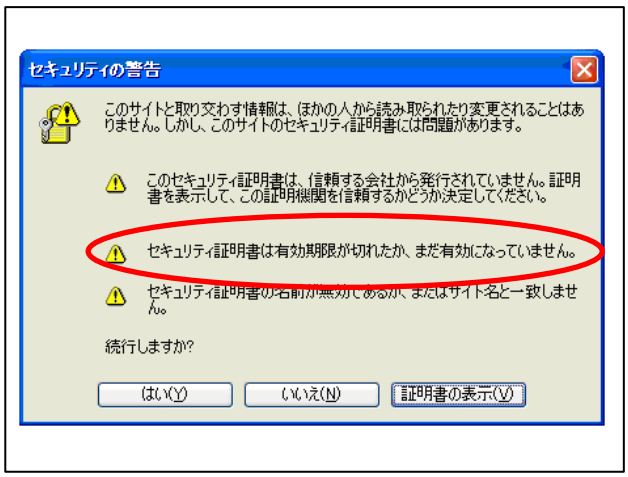


図 4.2-8　アドレスバーが表示されない事例

（8）証明書の期限切れ

SSL で用いられる証明書には、セキュリティ上、使用暗号の危殆化等に対応するために一定の有効期間が設けられている。証明書の発行先組織/会社は、有効期間を過ぎた証明書について証明書発行機関による更新手続きを受ける必要がある。本事例は、この有効期間経過後も証明書を更新しないで使用し続けている例である。有効期間切れの証明書を使用しているホームページのセキュリティは検証されていない場合があり、安心してアクセスできない。

なお、本事例の場合、IE6 では以下の警告画面が出る。



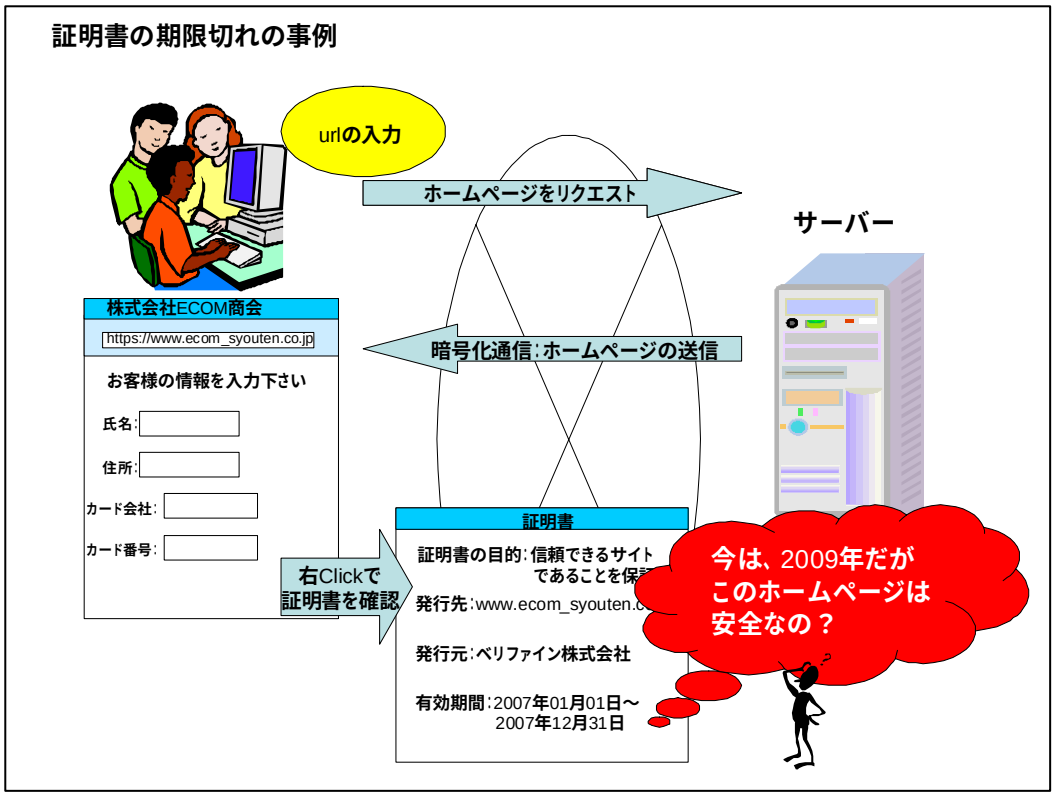
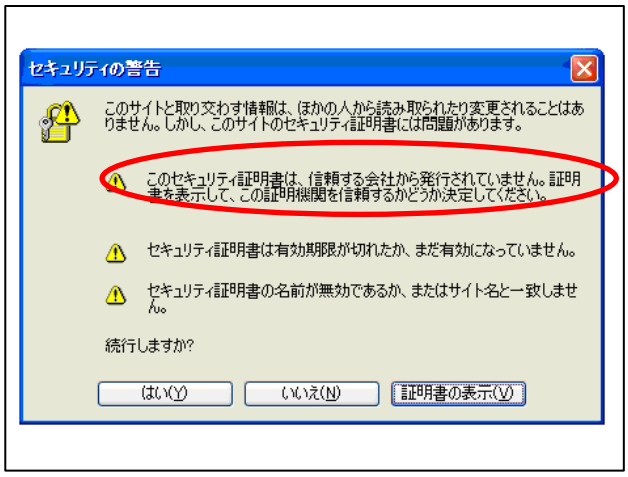


図 4.2-9　アドレスバーが表示されない事例

（9）自分自身で発行した証明書を使っている

本事例は、正規の証明書発行機関ではなく、自分自身で発行した証明書を使用している例である。通称、オレオレ証明書ともいわれている。ホームページ運用者（サービス提供者）の SSL 認証におけるセキュリティ保証の仕組みに対する知識不足や、社内のイントラネット用に開発したホームページの流用が原因として考えられる。認証書は、信頼できる第三者が発行して、初めて認証書としての効力を発揮できる（特殊な事例として、信頼できる機関が自分自身を認証するケースがあるが、ここでは詳述しない）。社内のイントラネット用のホームページでもない限り、自分自身の信頼性を自分自身で保証しても、何の効力もなく、ホームページのセキュリティは保証されない。なお、本事例の場合、IE6 では以下の警告画面が出る。



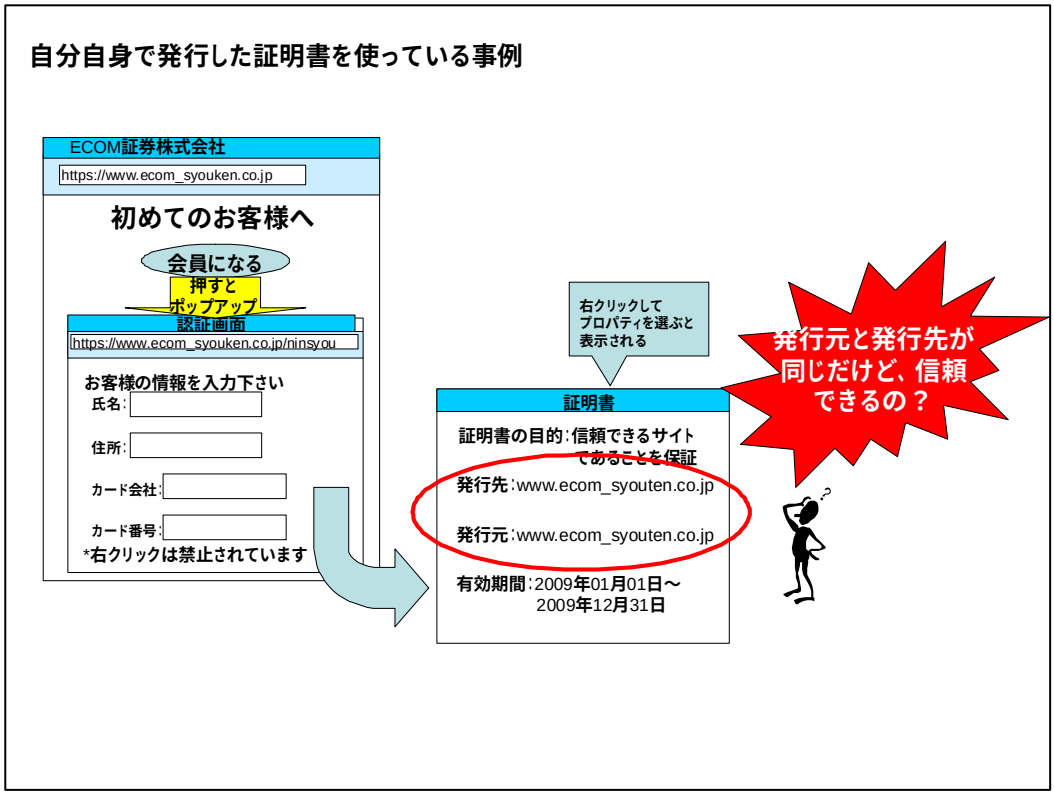
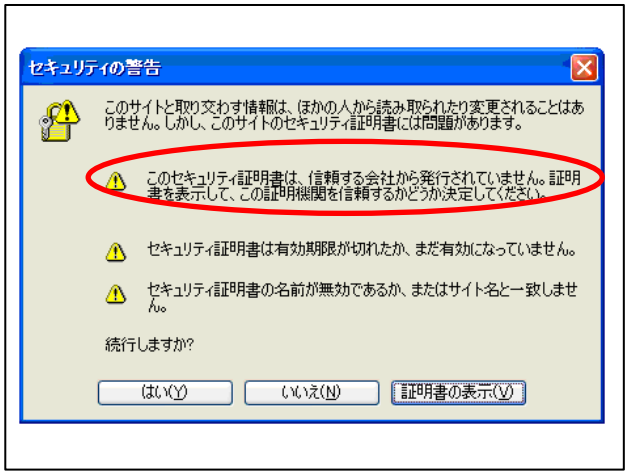


図 4.2-10　自分自身で発行した証明書を使っている事例

（10）信頼できない発行元が発行した証明書を使っている

本事例は、前述の自分自身で発行した証明書を使っている事例とよく似ているが、証明書発行機関がブラウザに登録されていない（信頼されていない）事例である。一般的に、ブラウザには一部の例外を除いて、信頼できる証明書発行機関が登録されている（信頼できる証明書発行機関であっても、ブラウザ提供元に認知されておらず、登録されていないケースがある。随時、ブラウザのバージョンアップ等で追加・修正が加えられている）。ブラウザに登録されている信頼できる証明書発行機関は、例えばIE6の場合、インターネットオプションのコンテンツから参照することができる。なお、本事例の場合、IE6では以下の警告画面が出る。



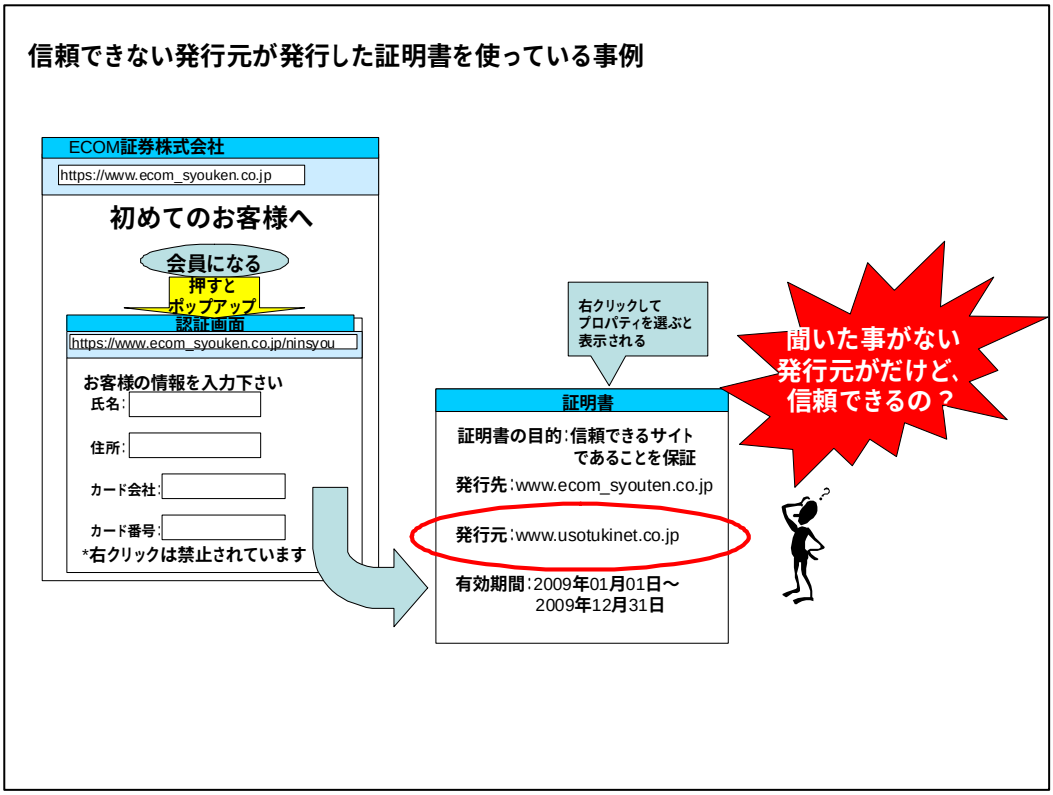


図 4.2-11　信頼できない発行元が発行した証明書を使っている事例

4.3. 運用/利用方法の考察

4.3.1. サイト運営のポイント

以下に調査事例からフィードバックされるサイト運営時のポイントをまとめる。

（1）アドレスバーやステータスバーは表示する事

調査事例では、アドレスバーやステータスバーを非表示にしているケースが散見される。アドレスバーの確認は､利用者がアクセスしている HP の真偽を確認する上で重要である｡また、ステータスバー上には、https を使用していることを示す鍵アイコン（証明書の閲覧にも利用）が表示される。これらから、アドレスバーやステータスバーを非表示とするべきではない。また、右クリックの禁止も、証明書の閲覧を妨げる事から行わないようにすべきである。

（2）重要な情報を入力する画面では https を使用する

http を用いた画面では、画面そのものや利用者の入力した内容等、入出力全てについて保護されない。このため、個人情報やユーザーID/パスワード等の重要な情報を入力する画面には https を適用すべきである。また、調査事例にもあったが、入力画面を http で提供して入力内容を内部的に https サーバーへ送信（post）している場合、入力画面そのものの改竄（例えば、送信先（post）の書き換え）に対処できないため、画面全体を https で提供すべきである。

（3）サービス提供者のドメイン名を使用する

ドメイン名は、利用者が正しいサイトにアクセスしているかどうかを見分けるための非常に重要な手がかりである。利用者が画面を移動する際に、ドメイン名が変わってしまうとフィッシング詐欺との見分けがつかない。ドメイン名はサイト全体でサービス提供者のドメイン名で統一すべきである。重要項目の入力画面を外部委託する等でやむをえずドメイン名が変わってしまう場合には、ドメイン名が変わる前の画面にその旨を記載すべきである。

（4）証明書を正しく維持する

証明書は、利用者がホームページの信頼性を確認する上で重要なものである。証明書記載の内容に変更があった場合や、証明書の有効期間が切れてしまった場合には速やかに証明書記載の内容を更新（有効期間が切れている場合には証明書自体の更新）すべきである。

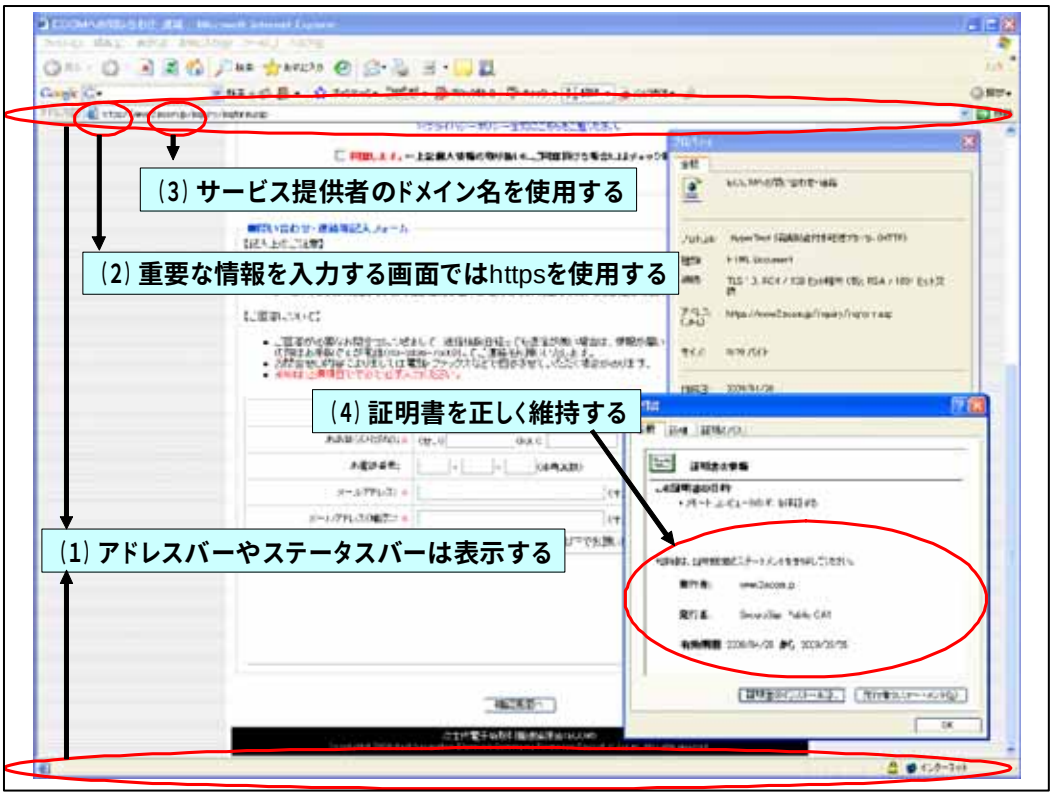


図 4.3-1　サイト運営者が注意するポイント

4.3.2. 利用者が確認すべきポイント

以下に調査事例からフィードバックされる、ホームページにアクセスする際に利用者が確認すべきポイントをまとめる。

（1）アドレスバー（ドメイン）、鍵マーク等

個人情報やユーザーID/パスワード等の重要な情報を入力する際には、入力画面のアドレスバーやステータスバーの鍵マークから、入力画面が本当にサービス提供者のものか、https によって保護されているかどうかを確認すべきである。ここで、入力画面で確認すべきとしたのは、最初にアクセスしたページがサービス提供者のものであったとしても、画面を移動して入力画面に至る間に https による保護の状況が変わっている場合や、全く違うドメインに誘導されている場合があるからである。

（2）証明書の内容

基本的に、有効期限や証明書の発行元、発行先についてブラウザが自動的に確認して、問題がある場合には警告してくれるが、初めて訪れるサイトや何らか不審に感じた場合には、利用者自らが証明書の内容を確認すべきである。

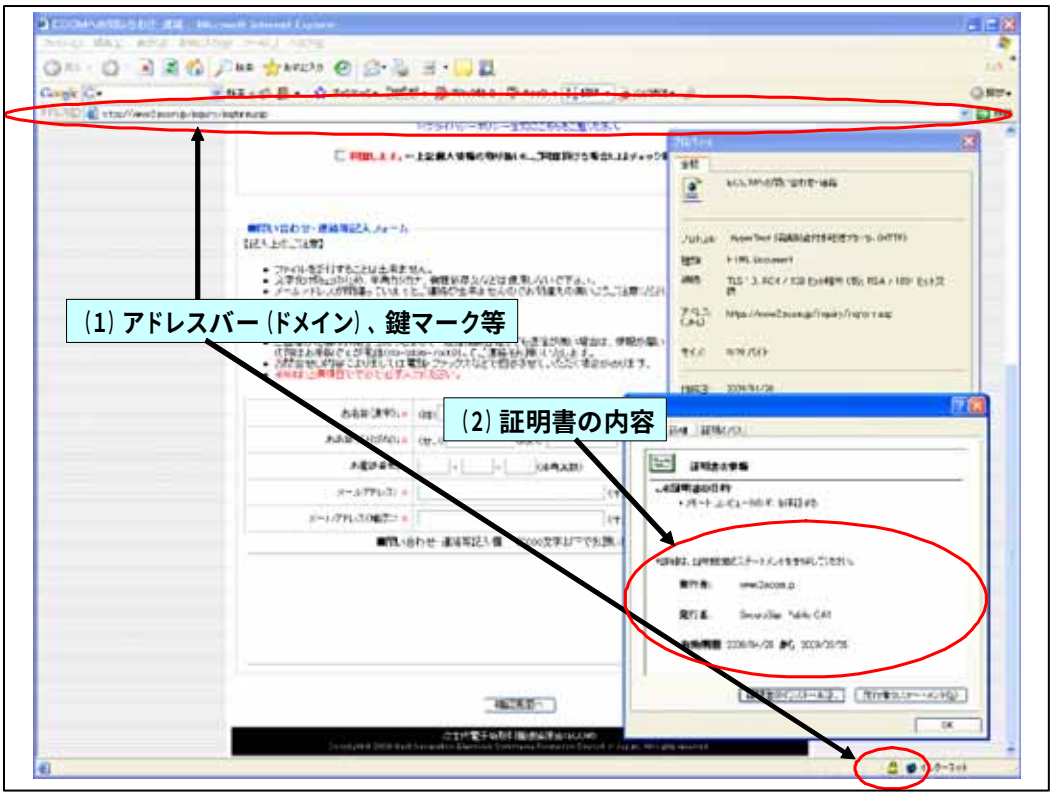


図 4.3-2 利用者が確認すべきポイント

4.4. まとめ

現在インターネットでは、ネットオークションや通信販売、銀行取引等、誰もが居ながらにして様々な商取引を行なえる状況となっている。インターネット上での商取引の技術は今後もますます向上し、さらに利便性を増すと考えられる。しかしながら、それに付随して浸透すべき利用者保護、すなわちセキュリティへの取り組みレベルは、技術的にも利用者への周知の点からも必ずしも満足できるレベルとは言い難い。IE7 や EVSSL の登場により、若干ではあるがサイトの安全性を確認しやすくなってきているものの、広範に及ぶ利用者層からみると、もっと簡便に安全確認できる仕組みの登場が心待ちされるところである。今後、商取引の端末が PC や携帯電話にとどまらず、テレビ等の家電製品への広がりが想定されることから、暗号通信・UI における革新的な技術が望まれるところである。

4.5. 付録 PKI と SSL

(1) PKI の概要

PKI とは、Public Key Infrastructure（公開鍵暗号基盤）の略で、正しい相手とのセキュアな通信を実現するための基盤のことである。PKI では通信の相手が正しい相手であることを証明するために、信頼できる証明書発行機関（認証局）が発行した証明書を使用する。

PKI は上記の、認証局、証明書及び、証明書を利用者に配布する仕組み（リポジトリ）から構成される。具体的には、

- 認証局：サーバーアプリケーション（市販されている）
- 証明書：規格（X.509）に定義される構造を持ったファイル
- リポジトリ：証明書を配布するための Web サーバーや FTP サーバー、LDAP サーバー等

である。PKI を活用したアプリケーションには、本報告で触れた SSL の他に S/MIME（電子メール）等がある。

(2) 証明書の役割とセキュアな通信の仕組み

証明書は鍵の入れ物の役割を担っており、認証局（発行元）、発行先（証明される企業/組織等）、有効期間等の情報の他に、鍵（公開鍵）を内包している。この公開鍵は証明書の配布とともに一般に公開されるが、公開鍵を使って暗号化した内容は秘密鍵と呼ばれる特別な鍵を使わないと復号化できない。

SSL の場合を例にとると、

① 利用者がホームページのアドレスを入力すると、Web サーバーから証明書が利用者の PC に送信される。
② PC で今回の通信に使用する鍵（共通鍵(*1)）を乱数を使って作成し、作成に使用した乱数を証明書に含まれる公開鍵で暗号化して Web サーバーに返す。
③ Web サーバーでは秘密鍵を使って PC から送られた乱数を復号化し、復号化した乱数から共通鍵を生成､生成した共通鍵を使ってホームページの内容(html ドキュメント)を暗号化し、PC に送信する。
④ このホームページに対して利用者が入力した内容等は、共通鍵を使って暗号化され、Web サーバーに送信される。
⑤ Web サーバー側では共通鍵を使って利用者の入力内容を復号化する。
⑥ 第三者は、証明書の鍵に対応した秘密鍵を持たないため、通信に利用されている共通鍵の内容が判らない。このため、盗聴したとしても通信内容の復号化が行えない。

といった PKI に共通鍵暗号方式(*1)を加えた仕組みでセキュアな通信を実現している。従って、秘密鍵さえ漏洩しなければセキュアな通信が行えるのである。

以下に SSL を用いた通信の概要図を示す。

*1：共通鍵は、共通鍵暗号方式と呼ばれる暗号通信の仕組みで使われる鍵である。共通鍵暗号方式では、通信する者どうしが同じ鍵（共通鍵）を持ち、この鍵で通信内容を暗号化して通信を行なう。共通鍵暗号方式では、どのようにしてセキュアに鍵を相手に届けるかが課題となる。

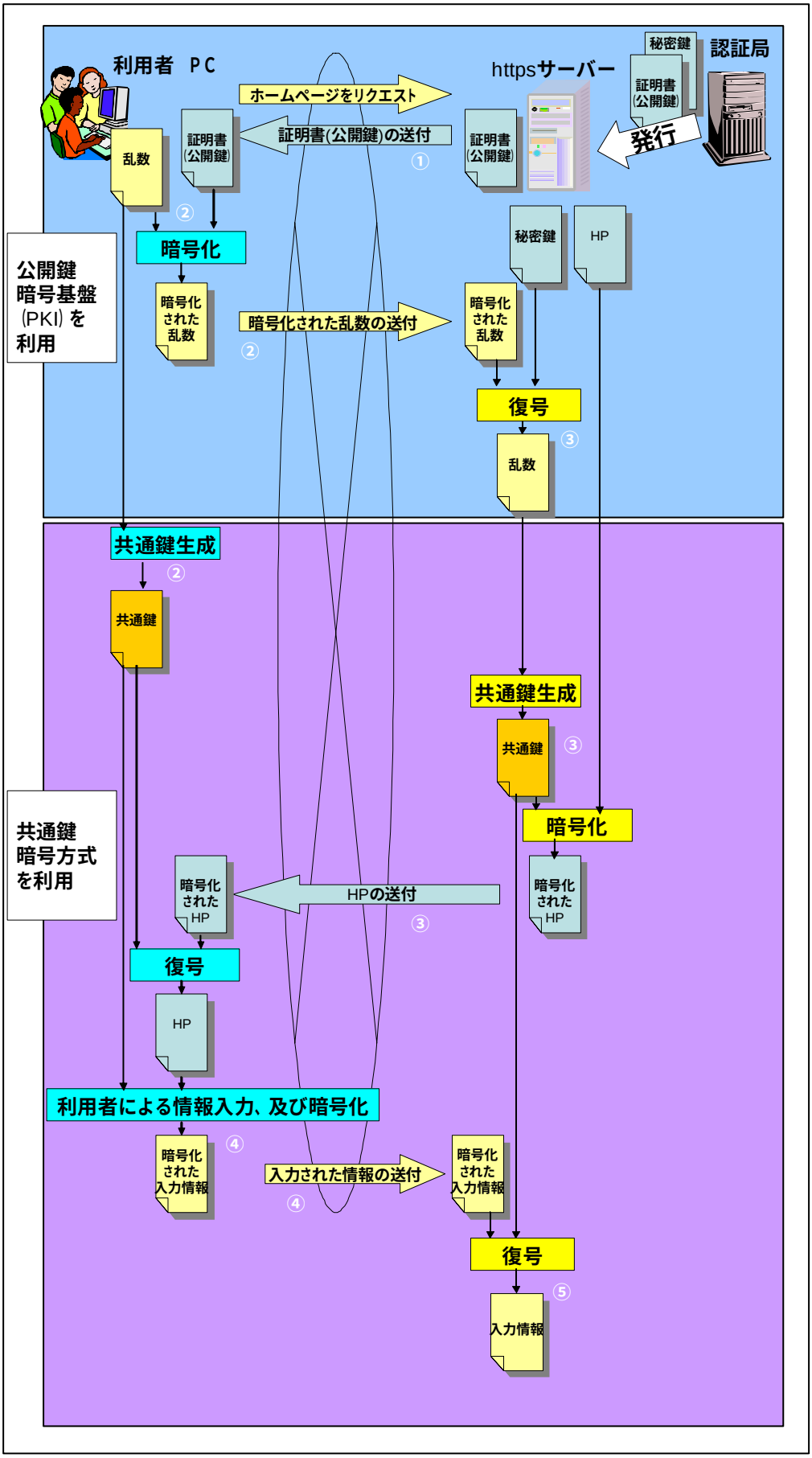


図 4.5-1　SSL を使った通信の概要

(3)　認証局の重要性

PKI の仕組みでは、鍵（証明書（公開鍵）・秘密鍵）を発行する認証局（発行元）の信頼性が最も重要なポイントとなる。認証局は、サーバーアプリケーションの一種であり、購入すれば誰でも鍵（証明書（公開鍵）・秘密鍵）を発行できてしまう。従って、利用者にとって証明書に記載される発行元が信頼性の高い認証局であるかどうかを確認することが、セキュアな通信を行う上で重要な事項となる。一般的なブラウザである IE や FireFox 等では、信頼される認証局のリストを持っており、利用者に代わって認証局の確認を行っている。また、本報告では詳述しないが、証明書には用途や目的別にいくつかの種類が存在する。利用者が、証明書に対する正しい知識（本報告では詳述していない）なしにブラウザに含まれる認証局のリストを正規のアップデートを経ずして追加・更新することは、信頼性の低い認証局が発行する鍵を認める結果となる可能性のある非常に危険な行為である。

PKI 適正運用･利活用 SWG（SWG3）メンバーリスト

（敬称略）

参加区分	氏名	会社名
会員メンバー	白木　勝	株式会社インテック
	保倉　豊	グローバルフレンドシップ株式会社
	川城　三治	グローバルフレンドシップ株式会社
	白川　昭久	（株）シーピーデザインコンサルティング
	上畑　正和	セイコーインスツル株式会社
	浅野　敬	株式会社帝国データバンク
	能勢　健一朗	東芝ソリューション株式会社
	高瀬　秀一	電気事業連合会
	武内　真弓	株式会社富士通総研
	玉田　竜一	富士電機ホールディングス株式会社
	宮地　直人	有限会社ラング･エッジ
有識者	辻　　秀一	東海大学
	荒川　一彦	近畿大学
	成瀬　一明	株式会社　東芝
	岩田　修	オフィス　イワタ
	高橋　和博	株式会社テプコシステムズ
	垣内　伯之	日本情報処理開発協会
オブザーバー	清水　友晴	経済産業省 情報セキュリティ政策室
	和田　浩明	経済産業省 情報セキュリティ政策室
SWG リーダ	再起　和夫	パナソニック株式会社（WG 主査）
事務局	合原　英次郎	次世代電子商取引推進協議会
	川嶋　一宏	次世代電子商取引推進協議会

5. データフォレンジック活用策検討 SWG 活動報告

5.1. 活動概要

5.1.1. 目的

近年の企業を取り巻く情報セキュリティ環境を考慮すると、大きなポイントとしては、社内コンプライアンスや情報セキュリティガバナンスという観点から見た J-SOX 法へ対応と、今後、政府の政策の目玉として設置が予定されている消費者庁との関連では、消費者保護への対応が挙げられる。

つまり、電子商取引としてのセキュリティを考えた場合、何らかのトラブル発生で取引相手から訴えられた時の対応、つまり相手企業や取引相手の消費者からの訴訟を準備する必要がある。例えば B to B であれば発注元企業と受注先企業の間で注文数に違いがあるケースで相手企業から損害賠償を求められたり、また B to C であれば、消費者の注文数と Web サイトの受注数に違いがあるケースなどで消費者からの訴訟になる場合である。

また、訴訟対応という点では、企業内部で情報漏えいが発生した場合に、その安全管理責任を問われるケース等が想定できる。これは、漏洩企業が安全管理について自身の無過失を立証できる環境（電磁的証拠等）があると非常に有利である。

これらの課題検討については、デジタル・フォレンジックという観点から、様々な電子証跡を残すにはどうしたよいのかという点で、電子商取引に適用できるガイドライン的なものを、EC データの証拠性という意味で「EC データフォレンジック」をテーマに検討したいと思う。

5.1.2. 活動方針

- デジタル・フォレンジックそのものに関する理解と共通認識の醸成
- 既存ガイドラインの内容検討（国内）と海外関連ガイドラインの翻訳検討
- EC データの証拠性という意味で「EC データフォレンジック」への適用可能性の検討
- 「EC データフォレンジック」ガイドライン策定に向けた項目検討

5.1.3. 活動経過

活動経過は表 5-1 の通りである。

表 5-1 データフォレンジックSWGの活動経過

期日	活動内容
平成 20 年 6 月 13 日	データフォレンジック SWG オリエンテーション
	・データフォレンジック活用策検討
7 月 31 日	第 1 回データフォレンジック SWG（SWG4）
	・「データフォレンジックと企業・消費者保護の関連検討」について ＜企業におけるデジタル・フォレンジックの基本的な考え方＞
9 月 24 日	第 2 回データフォレンジック SWG（SWG4）
	①有識者講演「内部統制評価に有効な証跡管理（エンタープライズ・フォレンジック）の研究開発」日立システム開発研究所、甲斐研究員） ②事務局より NIST ガイドラインの部分翻訳ご紹介
11 月 18 日	第 3 回データフォレンジック SWG（SWG4） ・SWG の提言内容と報告内容（目次、纏め方）について

5.1.4. 活動内容

（1）デジタル・フォレンジックの定義について

第 1 回目の SWG においては、まずデジタル･フォレンジックとはという定義からスタートした。そして、中心となるフォレンジック（forensic）という言葉のもつ意味として、一般的には「法廷の～」とか「法医学の～」といった意味の形容詞であり、フォレンジックスという名詞になると「鑑識課」「科学捜査」などの意味 である。

したがって、デジタル・フォレンジックとは、発生事象の証拠保全や不正アクセスの追跡手段を含む、 セキュリティ・インシデント発生後の「証拠保全」「解析」「証拠提出」の機能持合せたものということができる。（図 1）

図 1. デジタル･フォレンジックの必須「証拠保全･解析･証拠提出」

次に、デジタル・フォレンジックの種類であるが、大きく分けて 2 種類（製品群）に分類できる。まず、1 つ目の「ネットワーク・フォレンジック」であるが、これはネットワークを流通する全パケット（単位）取得し、解析しようとするものである。

2 つ目の「コンピュータ・フォレンジック」については、直接に特定のクライアント PC やサーバーの HDD 内のデジタル情報を調査するものである。
つぎに、それぞれの解析上の大きな違いであるが、 前者「ネットワーク・フォレンジック」については、取得パケットのネットワーク機器通過経路まで解析可能であり、挙動不審な動きをする不正端末を特定することができる
後者の「コンピュータ・フォレンジック」は、対象となる HDD を証拠用と解析用の 2 つ複製し、解析用で消去内容の判別可能化や証拠データの特定や保全を行う。
これらの、ネットワーク・フォレンジック（ログ解析,不正端末特定）と コンピュータ・フォレンジック（特定端末直接調査）の 2 つは、フォレンジックの両輪と呼ばれている（図 2)。

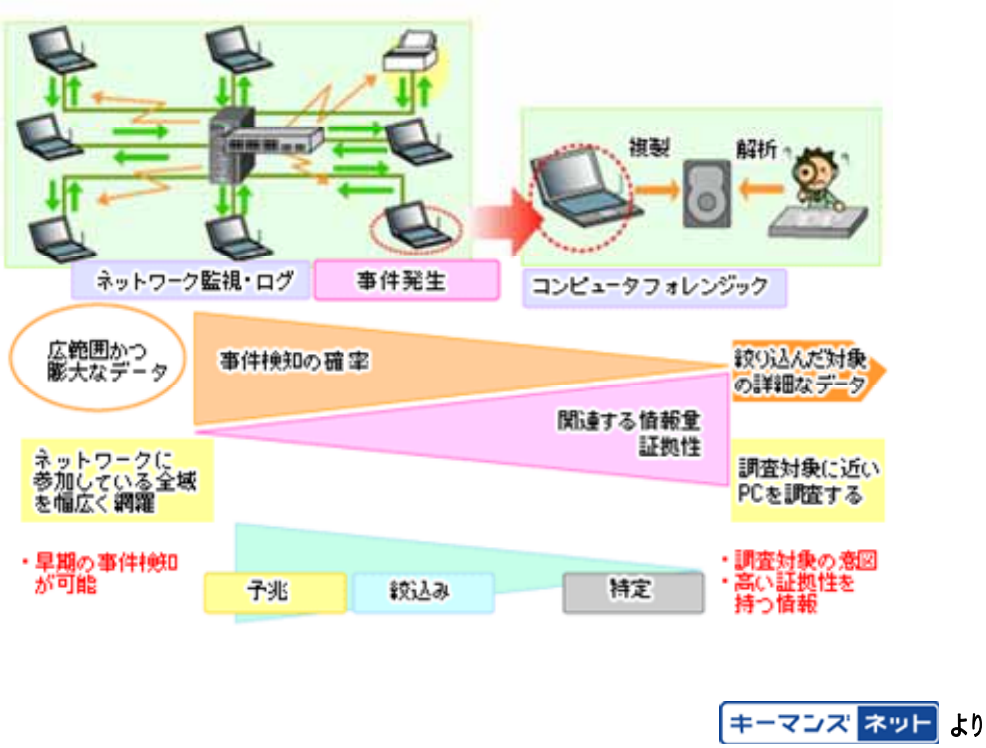


図 2. フォレンジックの両輪

（2）ネットワーク・フォレンジックの仕組み

つづいて各々の仕組みであるが、まずネットワーク・フォレンジックについては、管理範囲内のネットワークにフォレンジック・ツールを配置して、パケット取得や不審な挙動の端末を検知した上で、管理者に警告し、さらに端末操作ログも追跡可能である。また従業員に事前に当該ツールを設置する旨を伝えることで、内部犯罪の抑止効果も期待できる（図 3)。
そして、詳細な目的別のツール配置（設計）方法としては、次のように様々な手法があり、実際にはこれらをピックアップして組み合わせて利用することとなる。
例えば、HTTP の通信取得や、Proxy と LAN 間の IDS（不正侵入検知）やファイアウォール外側（スイッチに付属ミラーポート活用と、リピータハブや TAP 装置をネットワーク上配置接続の場合あり）チェック等が挙げられる。

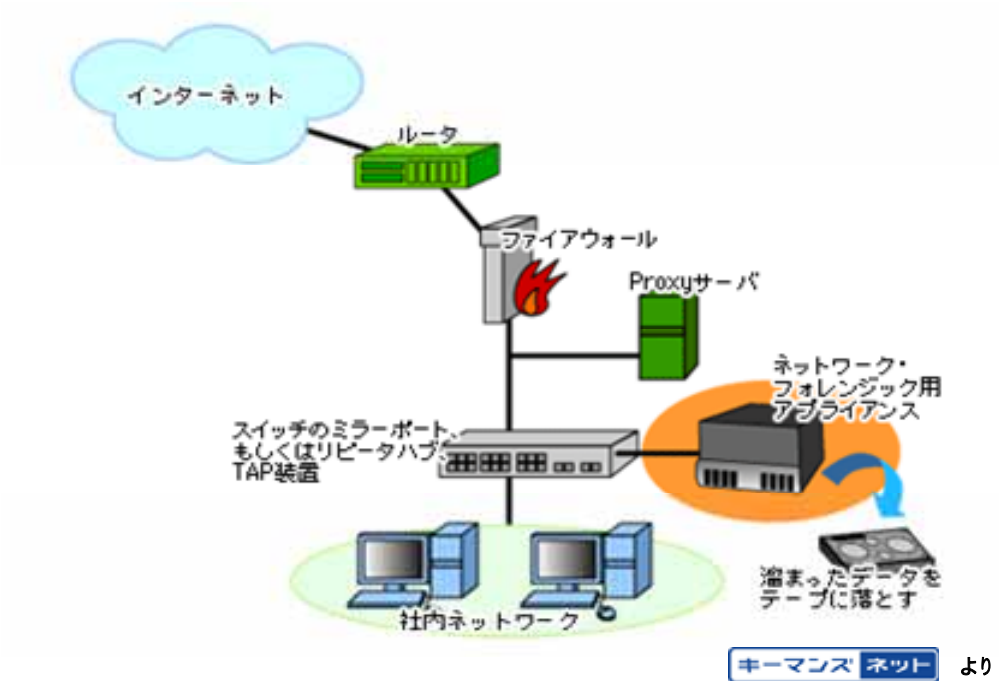


図 3. ネットワーク･フォレンジック

（3）コンピュータ・フォレンジックの仕組み

つぎにコンピュータ・フォレンジックについては、容疑者利用 PC の HDD を解析し、証拠保全するものである。但し、証拠保全の作業や解析手法はかなりのノウハウが必要ため、ベンダーが提供するサービスを利用するのが良い。そして、セキュリティ・インシデント（漏洩事件）発生後の事後対応ツールとして活躍するケースが多い。（図 4）

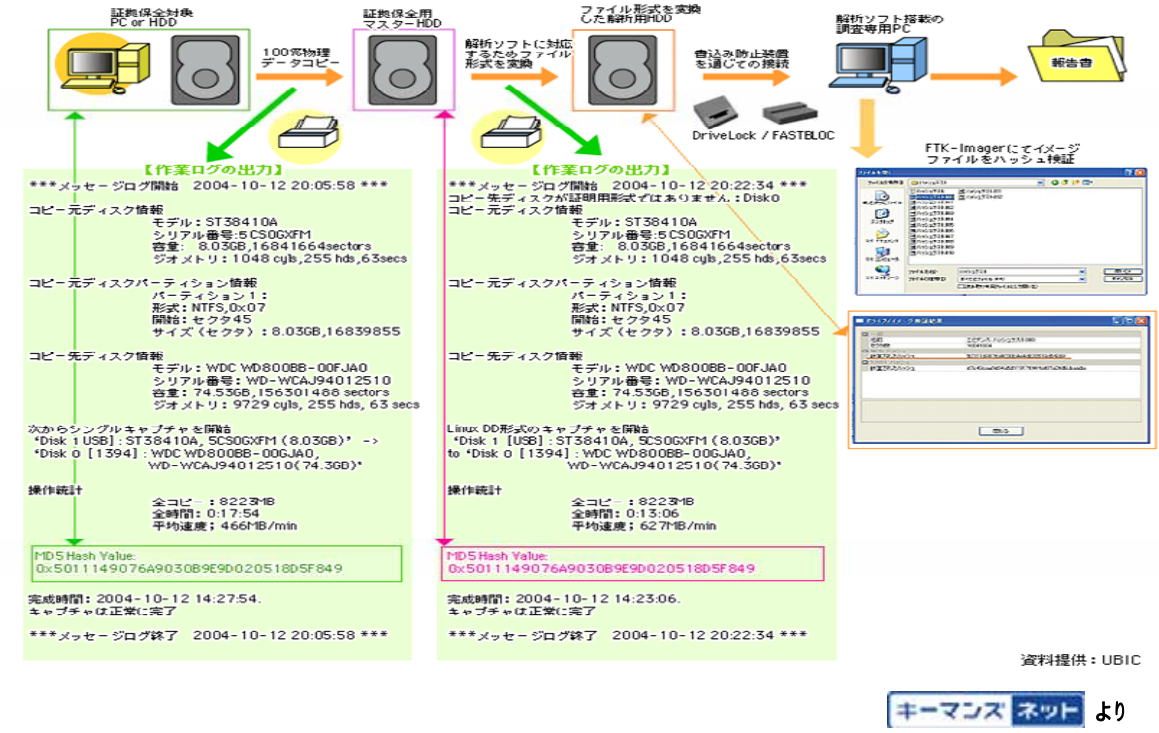


図 4. コンピュータ･フォレンジック

（4）証拠の収集順位がカギとなるコンピュータ・フォレンジック

対象＝ルータ、スイッチ、サーバー、クライアン PC、プリンタ等情報システム上ノードを調査

〇作業方法①：オフライン方式

サーバーやクライアント PC 等の調査対象ディスク・イメージを作成、調査専用ホストで解析調査用ホストには、信頼できる各種コマンドとツールを用意

〇作業方法②：オンライン方式

信頼できる調査用コマンドやツールを使用、対象マシンやデバイス上で直接証拠となるデータの収集・解析（注意：作業自体が肝心の証拠を破壊する可能性あり ）

〇特色：実行方法と、作業コマンドやツール選定は、自社の環境に応じて決定（図 5）

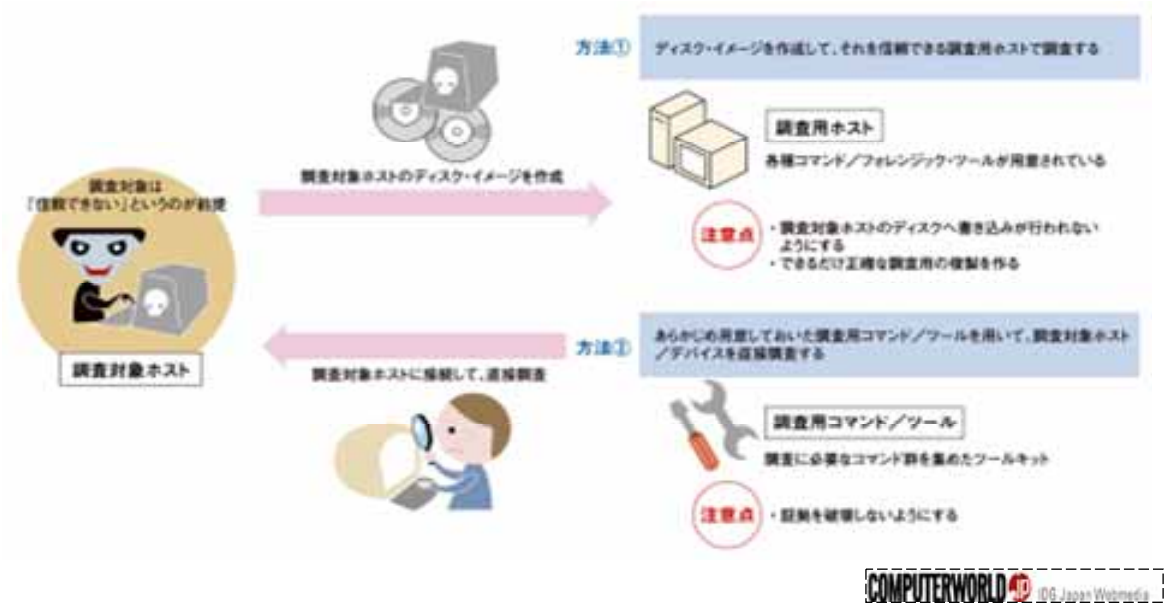


図 5. コンピュータ･フォレンジック作業方法

＜収集する証拠＞

〇マシン・デバイス等調査対象が多く、さらに証拠収集すべきデータの種類も多岐。

〇問題：どの種類のデータから集めればよいか。

RFC 3227 として規定：「証拠収集とアーカイビングのためのガイドライン」

「2.証拠収集における揮発性の順序」という項目で、収集すべきデータとそれらを収集する順番が示されており、これを参考とする（図 6）。

⇒揮発性の高いデータから収集を行うべき 、タイミングを見計らわないと取得不能情報も含む

「対象システムは 100%侵入者の支配下にある」認識必要。ログイン・プロセスや証拠保全コマンドの置換え、調査行動伝達プログラムやバックドア起動のおそれ。侵入証拠抹消の隠蔽プログラム仕掛けに気をつける。

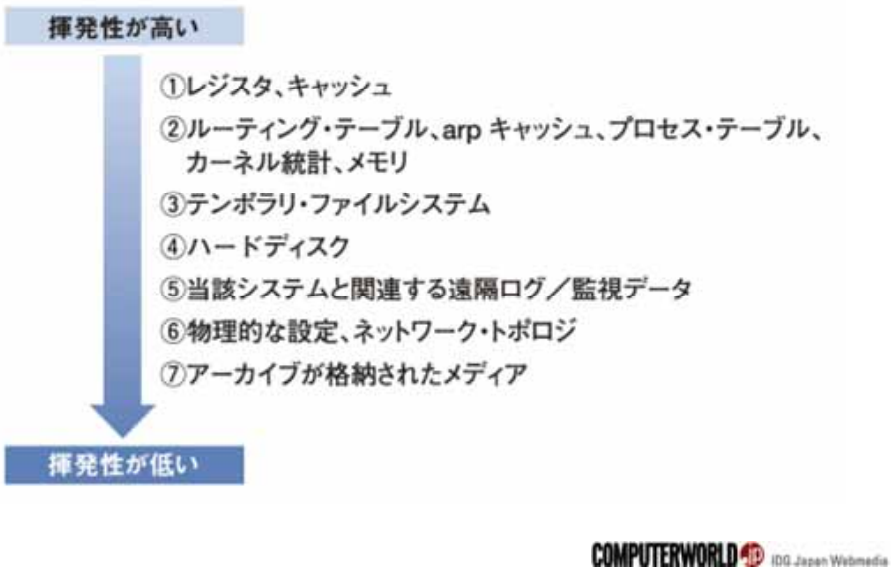


図 6. 証拠収集における揮発性の順序

（5）データの扱いに注意を要するネットワーク・フォレンジック

ネットワーク・トラフィックを調査対象、通常のトラフィックを記録する装置設置、そのデータ解析 ⇒対象システムにおける証拠をシステム外で保管可能、証拠の確保という点で有効

1.利用するツール

〇UNIX や Windows 等で利用のネットワーク・トラフィックのモニタリングツールにてデータを収集（サーバー・マシンを使用可能、ツール利用は高トラフィック環境でのデータ取りこぼし等の問題）

〇フリーツールの提供機能に付加価値を付けた商用製品もあり、以下のような特徴

・特定のプロトコルの再構築が行える

・収集するデータ量に応じて、ストレージ容量を拡張できる

・ネットワーク・キャプチャの性能が高い

・データ分析に便利な機能、強力な検索機能を備えている

・データの取り扱いを容易にするインターフェースが提供される

2.ネットワーク・トラフィックを扱う際の「配慮」

基本的に、ネットワーク上のトラフィックがすべて記録される。

トラフィックには、従業員の個人情報等プライバシーデータが含まれている可能性

また、従業員に関する情報を取得するという時点で、プライバシーの侵害に当たる可能性。

ネットワークの監視は、監視対象が企業・組織によって運用管理されるネットワークであれば、過去の裁判では基本的に認められているケースが多い

監視実施には、「監視に関するポリシー」で使用者による『労働者のモニタリング』の方針等を明確に提示しておく配慮や準備が必要

さらにデータの取得、保存、管理などデータの取り扱いに関しても十分な注意が必要、

ネットワーク上のすべてのトラフィックが記録される、収集データの中には組織のセキュリテ

ィ・ポリシー上、機密情報が含まれる可能性。
ネットワーク・フォレンジックの実施にあたっては、既存のプライバシーや機密情報の取り扱いなどに関する各種セキュリティ・ポリシーを確認し、それらにおいて、データの取得／運用管理にかかわるポリシー（取得する情報の範囲、最低限保存しておく必要のある期間、バックアップ／消去に関する事項など）に関して、不足している部分があれば、それを明確に定めておくといったことが必要。（表 5-2.5-3）

表 5-2.5-3：各フォレンジックの特徴

表 5-2　コンピュータ･フォレンジックの特徴

長所	・対象を直接調査することで、より正確にノードの状況を把握できる
短所	・取得した証拠自体がすでに侵入者によって改竄されている可能性がある ・調査活動が証拠破壊につながるおそれがある

COMPUTERWORLD.jp IDG Japan Webmedia

表 5-3　ネットワーク･フォレンジックの特徴

長所	・調査対象のノードに直接アクセスすることなく、外部から調査することができる ・対象のネットワークにおけるトラフィックを外部から調査し、情報を収集するため、取得した情報を証拠として記憶媒体に保存することが比較的容易である
短所	・暗号化されたトラフィックは解析ができない場合が多い ・トラフィックが大量にわたる場合、取りこぼしが発生する可能性がある ・プライバシーの侵害に抵触する場合がある

COMPUTERWORLD.jp IDG Japan Webmedia

（6）インシデント・レスポンスの一プロセスとして実施
●フォレンジック＝訴訟・情報漏洩対策手段として、組織・人・物理面等複数の側面取組必要
⇒個々に検討よりも、インシデント・レスポンス（IR）の一プロセスとしてとらえる必要あり
●フォレンジック導入はいきなり製品選定からではなくまずは、　（IR）体制／計画の構築・見直し⇒そのうえで、技術面に偏ることなく運用管理も踏まえ、組織にとって実行可能かつ最低限必要なレベルから、フォレンジックに取り組み。

（7）デジタル・フォレンジックツールの抽出（デジタル・フォレンジック事典より）
1.「ネットワーク・フォレンジック・ツール」　＝ネットワーク流通全パケット取得・解析
：取得パケットのネットワーク機器通過経路まで解析、挙動不審不正端末を特定
①電子メール関連
・メールフィルター

・メールアーカイバ
②ログ情報関連
・広域ログ監視ツール
・サーバーログ監視、保護ツール
・クライアント PC ログ管理ツール
・ログ保全、解析ツール
・ログ管理、監査ツール
③その他
・パケット情報保全ツール

2. 「コンピュータ・フォレンジックツール：証拠保全用ハードウェア」
＝直接 PC やサーバーの HDD（情報）調査
：対象 HDD を証拠用と解析用 2 つ複製、解析用で消去内容判別可能、証拠特定、保全
① ハードディスク消去ツール、②データ複製ツール、③書込み防止装置

3. 「調査・解析用ツール」
＝ハードディスク・ファイルシステム対象：①取得②解析③報告の 3 機能
：ブラウザ履歴・キャッシュファイル解析・ファイル形式変換と DB 作成・パスワード解析・レジストリー保護領域の調査

4. 「解析専用コンピュータ」＝証拠データの高速保全・解析業務の共有
以上がデジタル・フォレンジックのツール群である。

5.2. EC（電子商取引）の観点からみたデジタル･フォレンジック有効性

「民事証拠法から見たデジタル・フォレンジックの効用」（南山法科大学院教授：町村泰貴氏の論文より抜粋・編集したものを以下に記すものとする。）

5.2.1. 消費者保護から見たデジタル･フォレンジック効用

EC（電子商取引）上の観点からみたデジタル・フォレンジックの有効性としては、EC デジタルデータを証拠提出することにより、デジタル媒体・プリントアウトの真正な成立を証明できることである。

1. 電子商取引（EC）上の取引記録の違い とデジタル・フォレンジックの効用
電子メール等の取引データが、送信側の保有データと受信側の保有データとで食違い、いずれが真正か確認の必要性があるというようなケースについてデジタル･フォレンジックが有効である。特に、仮に何らかの事由で取引相手企業が、故意に不利益になる受注取引の内容を改ざんをした場合である。また、別なケースとしては、通常のネットショッピング以外にも、多額のオンライン株取引、不動産売買、高額嗜好品等の取引においては、同様に内容改ざんが問題になることが

考えられる。
普通、Web 申込では、消費者側が証拠画面データを保存しないケースがほとんどであり、このため訴訟になったとしても、消費者自身の正当性を 通常手段で立証するのは到底無理である。
ちょうど、上記のような場合に、下記の例に挙げたフォレンジック技術を利用すれば真正成立が立証可能となる。
（例 1.）双方のコンピュータの利用履歴から改ざんの有無を明確化する、つまり筆跡鑑定に相当するフォレンジック鑑定を有効とさせる場合 。
（例 2.）EC 上トラブルの防止という観点から、デジタルデータ保有者（消費者）にフォレンジック技術で原本一致保証の自動バックアップを取らせる、つまり実質的証拠力十分なデジタル署名に代替可能なデジタルデータとする場合。

5.2.2. 企業自身のための EC フォレンジック技術利用

一般に企業が法令遵守下において、機密情報が漏洩してしまい、結果的に違法行為が発生して、第三者の他人が損害を受けて、損害賠償の義務が発生するケースがある。
同じく、電子商取引（EC）でも、何らか原因で履行障害が生じて、その賠償責任の有無が問われるケースがある。
そこでは、不法行為・債務不履行等の立証において、原則として無過失ならば、賠償義務を負わないことがそのポイントとなる。
つまり、不法行為責任を追及する側に立証責任があろことから、判断材料としての周辺情報を含めて、デジタル関連の諸情報に乏しい訴訟環境の中で、その是非を裁判所の微妙な判断に委ねる不安定さを企業としては、現状として覚悟せねばならない。
したがって、この訴訟時の証拠性を高めるためにも、企業としては、平時からデジタルデータの運用・保管が課題となってくる。
そして、リスク回避という観点からも、企業自身の持つ電子商取引データ（B to B、B to C 等含む）保管と、そのデータ信憑性・証拠性を高めることが重要となってきた。
ここに、電子商取引において、デジタルデータフォレンジックがこれから注目されるポイントがある。
こうして、フォレンジック技術の利用局面としては、万が一、他者から賠償責任を追及される場面において、被訴訟側としては、必要な注意を尽くしたこと、つまり無過失を保管データ・ログ等で立証することにより、、不測の損害を回避することが可能である。
さらにリスク・マネジメントの一環としてみれば、このデジタル・フォレンジックという万全の「備え」は、当面の発生した、責任追及の回避の決め手となるだけでなく、どうせやっても無理だと立証側に思わせること、すなわち提訴リスク自体を回避に繋がり、紛争予防効果があることを忘れてはならない。
今後、企業におけるデジタル・フォレンジックの課題としては、昨今の社内コンプライアンス対応や法令遵守の追求による、内部統制や j-sox 対応・事前の証拠開示を求めた e ディスカバリへの適応等がその特性にマッチしたものとしてあげられる。また、内部犯罪抑止力の向上に対しても、有効な手段となることは間違いない。
但し、その情報収集時におけるモニタリングの是非やプライバシー保護の問題等については、こ

れからの大きな課題といえよう、

5.3. EC（電子商取引）におけるデジタル･フォレンジックの適用課題

5.3.1. EC フォレンジックとしての考え方として適用課題

まず、その前提となる「企業におけるデジタル・フォレンジックの基本的な考え方」（デジタル・フォレンジック事典より抜粋）を見ていくものとする。

- デジタル・フォレンジックは IT 戦略策定時の重要課題である
- 当該コンプライアンス対策は、経営に組込む（ビルトインする）べきである
- 怠るとリスク許容を潜在化させ、事故発生時には、事業効率の相殺では済まない悪影響を与える可能性がある
- 経営層が IT 戦略策定時に組込み、各事業部局が IT 導入時にも組込む必要

これらを、EC フォレンジックとしての考え方として適用課題を検討すると下記の通りである

- デジタル・フォレンジックは EC 上の重要課題と位置づけ
- 当該コンプライアンス対策を、サイト設計・運営に組込むべき
- 怠ると訴訟リスク等を潜在化させ、事件・事故発生時には莫大なコスト発生により、経営の根幹を揺るがす可能性
- トップがサイト運営方針策定時に組込み、発注者（開発者）がシステム導入時にもブレークダウン・意識して組込む必要

以上が、「企業におけるデジタル・フォレンジックの基本的な考え方」の各項目である。

5.3.2. EC フォレンジックの対象となるデータとしての差異

前提となる一般的な「デジタル・フォレンジック対象データとしての違い」（デジタル・フォレンジック事典より抜粋）は下記の通りである。

①電子文書等＝内容が証拠として意味を持つ

- データの完全性が求められる
- データをありのままに保全しておく必要がある

②ログファイル等＝行為の記録発生の事実が証拠として意味をもつもの

- データの否認不能性が求められる
- データをそのままではなく形式変換しても構わない場合がある

注意：電子文書の当事者間だけでの原本性確保は困難であることを認識

つぎに、上記をベースに電子商取引に特化した EC フォレンジックの対象となるデータとしての差異を見ていくと次の通りである。

①Web からの申込み内容等＝証拠能力の保全

- データの完全性確保⇒電子証明・タイムスタンプ等の利用 （破壊・改竄・消去の防止）
- ありのままに保全の必要性⇒情報管理の用件（加工防止）

②ログファイル等＝行為の記録発生事実が証拠として意味保持

- データの否認不能性⇒注文意思確認後、当該データ送付確認
- 5 つの事項（発注内容・時刻・回数・行為者・受注者）の完全性

以上が、一般及び EC フォレンジックの対象となるデータとしての差異である。

5.3.3. EC フォレンジックを利用する立場による違い

前提となる一般的な「デジタル・フォレンジックを使う局面による違い」（デジタル・フォレンジック事典より抜粋）は下記の通りである。

①原告としての立場＝追求する立場

- 被害の事実を主張

②被告としての立場＝防衛する立場

- 加害の事実の誤りを主張＆加害の責任範囲の主張
- 行為者の別＝組織内の者による行為、組織外の者による行為
- 作為・不作為の別＝行為をしたこと、行為を怠ったこと

これによりフォレンジックの目的決定･手法が定まるため､事前対策を講ずることが可能となる。

つぎに、上記をベースに電子商取引に特化した EC フォレンジックの対象となるデータとしての差異を見ていくと次の通りとなる。

①訴訟する立場＝追求する立場

- 被害事実主張⇒（例）B to B：受発注データ違い＝損害発生企業

②訴訟される立場＝防衛する立場（B to B で受発注データの違いで訴えられた企業）

- 行為者の区別＝企業内部による行為、企業外（相手先）の行為
- 作為・不作為の別＝注文をしたのか、注文を怠ったことの証明か

以上により当該フォレンジックの目的により、企業としての取るべき手法の決定が可能となる。

5.4. 各種フォレンジック関連ガイドラインの紹介

5.4.1.「エンタープライズ･フォレンジック証跡管理ガイドライン」（日立 s/s 作成：考え方&概要説明）

●「内部統制評価に有効証跡管理（エンタープライズ・フォレンジック）の研究開発」研究成果（株）日立製作所：システム開発研究所、甲斐研究員より講演 ⇒以下 Contents

1 章　研究背景
2 章　研究目的
3 章　情報漏洩リスクから見た仮説検証
4 章　訴訟対応リスクから見た仮説検証
5 章　情報管理強化に向けた検討
6 章　研究成果の評価

●企業としての活用事例

①対：情報漏洩リスク＝（例）お客様情報流出の再発防止対策

②対：訴訟対応リスク＝（例）民事訴訟時に証拠開示対象、 従来の書類に、電子的情報が追加（米国：**eDiscovery）対応**

●考え方

「デジタル・フォレンジック」は情報セキュリティガバナンスの一環＝その手法の 1 つと考えるというのが、このガイドラインのベースとなっていると思われる

5.4.2. エンタープライズ･フォレンジックの実施手順

■情報の管理の強化の基本方針

①情報漏洩・訴訟対応に備えたルールを策定する

②漏洩させてはならない情報・証拠とないうる情報を識別する

③ルールの通りに情報を管理する

④ルールの通りに管理していることを確認する

1. ポリシー策定　2. 情報の識別　3. コントロール　4. .監 査

5.4.3. エンタープライズ･フォレンジック研究概要

・ 「コンピュータ・フォレンジック」と「ネットワーク・フォレンジック」適用

・事故発生後の正確調査（説明可能性）と未然防止対策（機密性）

・情報漏えい＆訴訟対応から見た管理策・実施手順・ガイド検討

以上の考え方を EC 上のデジタルフォレンジックガイドに適用検討し、電子商取引関連企業（サイト運営・ベンダー）の 「参考書・身近なバイブル」を目指すというものである。

5.4.4. NIST ガイドラインの検討

NIST：アメリカ合衆国の国立標準技術研究所(National Institute of Standards and Technology)

（1）Special Publication 800-86

「Guide to Integrating Forensic Techniques into Incident Response」概要

●定義＜デジタル・フォレンジック＞ とは

①データの特定、収集、検査、分析へ科学を応用

②情報の完全性を保ちデータに関する証拠保管の継続性を維持

●背景＜データ量の増加、データソース多様化＞

デジタル・フォレンジック技法⇒多数の目的（下記）で利用可能

①犯罪や国内政策違反の捜査、コンピュータセキュリティ事件の再構成

②運用上問題のトラブルシューティング、突発的システム損害からの復旧等

●必要性

事実上全ての組織が、デジタル・フォレンジックの実施能力を持つ必要性

本ガイド＝方針・手順策定を含め、フォレンジック能力確立の詳細な情報提供

（焦点＝コンピュータセキュリティ事件への対応を支援）

※本書はフォレンジック捜査の実行ガイド利用や、法的助言として解釈、犯罪活動捜査の基礎としては不適切（各組織で適用対象法律や規制が異なる）

本ガイドを、法律顧問、警察当局者、管理者から提供される広範なガイダンスと併せて、フォレンジック能力構築の出発点として活用望む

というのが上記の Special Publication 800-86 の概要である。

（2）Special Publication 800-101

Sponsored by the Department of Homeland Security

「 Guidelines on Cell Phone Forensics」概要

●定義＜携帯電話フォレンジック＞

一般に認知された方法を用い、フォレンジック上の健全な条件下で、携帯電話からデジタル証拠を回収する科学

●本ガイドの概要

①古典的な C フォレンジックでカバー不能な最新機能の携帯電話への見識深堀

②上記に関連する技術やその技術とフォレンジック手順の関係を説明

③携帯電話保存のデジタル情報の保全、入手、検査、分析、報告等の実施支援、
利用可能なフォレンジック・ソフトウェアツールに言及

●本ガイドの目的

①携帯電話取扱い適切方針と手順を諸関係者・各機関が進化させる一助

②携帯電話絡む新状況下、対処するフォレンジック専門家の準備体制整備

※但し、本書は法的助言と解釈されるべきではない。諸関係者・各機関においては本ガイドを、法律顧問、当局者、管理者から提供の広範な指針と併用してフォレンジック能力を発展させる出発点として活用いただくというのが上記の Special Publication 800-101 の概要である。

5.5. デジタル･フォレンジック･マネジメント態勢構築支援サービス

5.5.1. サービス内容

デジタル・フォレンジックの運用については、他のマネジメントシステムと同様に PLAN⇒DO⇒CHECK⇒ACTION のサイクルを回すことが大切である。したがってこの PDCA サイクルの確立のために体制構築が必須であり、そのデジタル・フォレンジック・マネジメント態勢構築の項目内訳は下記の通りである（図 7）。

①デジタル・フォレンジック・マネジメントポリシー策定支援

②デジタル・フォレンジックツール導入（選定）支援

③デジタル・フォレンジック教育支援

④企業活動の正当性証明支援

⑤e-Discovery 対応支援

⑥ホットライン等、内部通報態勢の構築支援

⑦インシデント・レスポンス対応手順書の策定支援

⑦　状評価支援

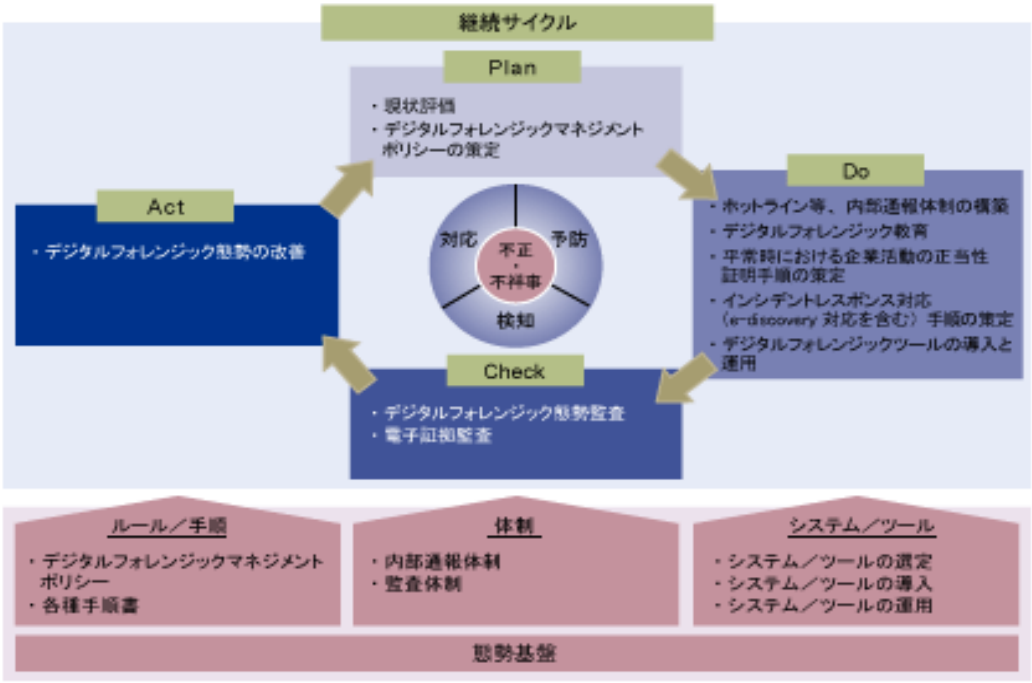
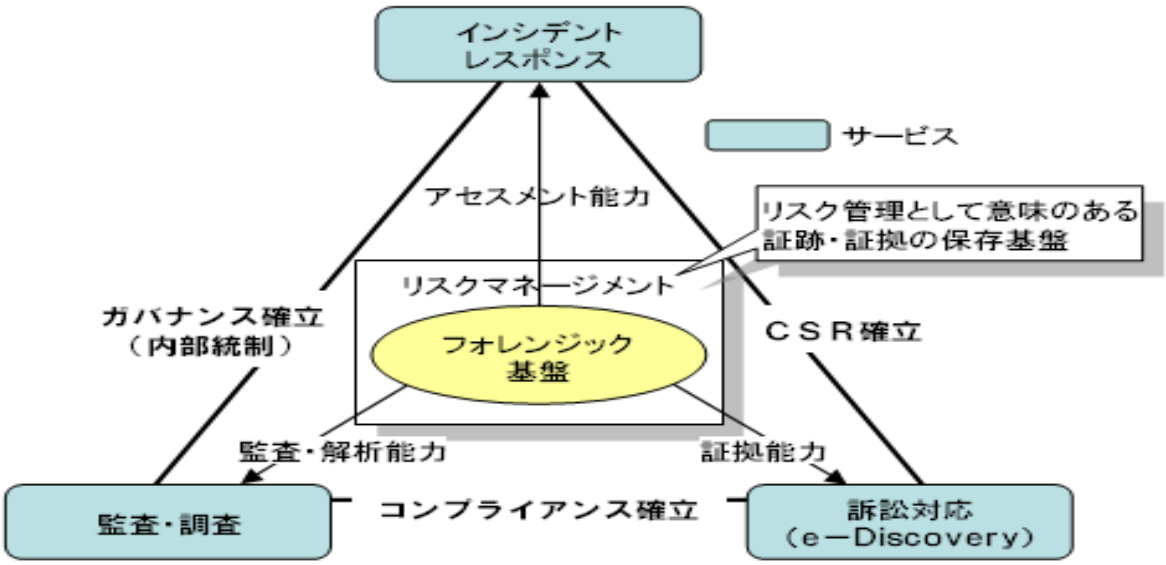


図 7. デジタル･フォレンジック･マネジメント態勢構築支援サービス

（KPMG ビジネスアシュアランスジャパン ＞IT アドバイザリーサービスサイトページより）

5.5.2. フォレンジック基盤を活用したサービス展開

企業経営の視点から、企業・組織には「CSR」が求められ、CSR を実現するために「ガバナンス」や「コンプライアンス」の確立が必要になっている。そのために企業にはあらゆるリスクに対するリスク・マネジメントが求められるが、その基盤となるのがフォレンジックになってくると考えられる。（図 8）



（セキュリティ対策コラム ©2008 NTT DATA SECURITY CORPORATION.）

図 8. フォレンジック基盤を活用したサービス展開

以　上

データフォレンジック活用策検討 SWG（SWG4）メンバーリスト

参加区分	氏名	会社名
会員メンバー	保倉　豊	グローバルフレンドシップ株式会社
	川城　三治	グローバルフレンドシップ株式会社
	高瀬　秀一	電気事業連合会
	織茂　昌之	株式会社日立製作所
有識者	辻　　秀一	東海大学
	荒川　一彦	近畿大学
	成瀬　一明	株式会社　東芝
	岩田　修	オフィス　イワタ
	高橋　和博	株式会社テプコシステムズ
	垣内　伯之	日本情報処理開発協会
オブザーバー	清水　友晴	経済産業省 情報セキュリティ政策室
	和田　浩明	経済産業省 情報セキュリティ政策室
主査	再起　和夫	パナソニック株式会社
事務局(リーダ)	合原　英次郎	次世代電子商取引推進協議会
	川嶋　一宏	次世代電子商取引推進協議会

■参考･引用文献 (順不同)

・南山法科大学院教授　町村泰貴：民事証拠法から見たデジタル・フォレンジックの効用
（http://www.digitalforensic.jp/archives/2004/Machimura.pdf）
・NIST（アメリカ合衆国の国立標準技術研究所）
:「Guide to Integrating Forensic Techniques into Incident Response」
（http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf）
・NIST：「Guidelines on Cell Phone Forensics」
（http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf）
・特定非営利活動法人デジタル・フォレンジック研究会：「デジタル・フォレンジック事典」
・「内部統制評価に有効証跡管理（エンタープライズ・フォレンジック）の研究開発」
（株）日立製作所：システム開発研究所、甲斐研究員：講演資料（2008.9.24）

■参照･引用サイト一覧 (順不同)

・特定非営利活動法人デジタル・フォレンジック研究会
http://www.digitalforensic.jp/
・これさえ読めば基本はカンペキ！「フォレンジック」
http://www.keyman.or.jp/3w/prd/71/30001771/
・プロアクティブ・セキュリティ──見えない敵に先手を打つ 第 10 回 フォレンジック［前編］
http://www.computerworld.jp/news/sec/22921.html
・プロアクティブ・セキュリティ──見えない敵に先手を打つ 第 11 回 フォレンジック［後編］
http://www.computerworld.jp/news/sec/23081-1.html
・KPMG JAPAN：リスクアドバイザリーサービス・IT アドバイザリーサービス
http://www.kpmg.or.jp/serviceline/riskadvisory/digital_forensic.html
・セキュリティ対策コラム　―ガバナンス時代の新たな波―デジタル・フォレンジックを基盤とした新展開＜第 2 回＞NTT DATA SECURITY CORPORATION
http://www.nttdata-sec.co.jp/article/security/080905.html
・「J-SOX 時代のデジタル・フォレンジック」とは
http://www.itmedia.co.jp/enterprise/articles/0701/17/news006.html
・デジタル・フォレンジックとは
http://itpro.nikkeibp.co.jp/article/Keyword/20070208/261376/

6. おわりに

近々の国内ネットワークセキュリティの現状傾向をみても、まだまだ P2P ファイル共有ソフトによる情報漏洩事件続発の問題は、依然として解決しておらず、 Winny や Share 利用ノード数も減少せず、暴露ウイルス情報流出による被害が後を絶たない。

また、報告書の前書きに記載があるように攻撃者が利用する舞台が、Web にシフトしてきており、さらに従来からの SQL インジェクションやクロスサイト・スクリプティングに加えて、DNS キャッシュ・ポイズニングや Hosts ファイルの書き換えや、いわゆる SEO ポイズニングといった新たな攻撃手法が蔓延している。つまり、アタックする側は益々巧妙に組織的な活動にシフトしてきている事実がある。

これに対する 情報セキュリティ保護の当面の課題及び対策については、この一年間の取り組みを通じて得られた結論としても、即効性のある効果的な対策は依然として無く、日頃からの地道な対応（パッチ当てやウイルスチェック等）がやはり基本であることは変わりない。ただ、各サブワーキング毎の取り組みの中に、これまで単一企業ごとや消費者個人に頼っていた情報セキュリティ保護を、企業間や企業・消費者間での共同ディフェンスに変えようとする努力の萌芽が出ている。これらの、企業や消費者が拠り所とする情報セキュリティ保護の共通バイブル（ガイド）のようなものができないかという取り組みを情報セキュリティワーキング全体として継続していかねばならない。

つまり従来からの、下記のような基本的（一般的）対策つまり受身的対策だけで本当に十分か？という問いに対する回答を見つける活動である。

- アンチ（ウイルス・スパイウェア・スパム）統合セキュリティソフト導入
- OS やソフトを常に最新状態（セキュリティパッチを適用する）
- 作成・配布元不明な実行ファイルや文書を不用意に開かない
- 不審メール添付ファイルを開封や（正規 URL も）リンククリックせず
- 利用サイトパスワードや SNS 等情報共有サービスアクセス設定を定期的見直し

以上のような、従来型のパッシブな（受動的）対策では、昨今のパワーアップした攻撃者対策としては不足であろう。最大の セキュリティホールは人であるという根本真理を前提として、より良いレベルの 安全安心な EC 基盤を築くためには、グループ・共同防衛構想ともいうべき情報セキュリティ対策が不可欠であり、前述の企業間や企業・消費者間の情報取引を保護する何らかの共通バイブル（ガイド）の策定を目指してアクティブな（積極的）活動を継続することが肝要である。

またさらに、その先の近未来を見据えた活動としては、安全・安心 EC グループでも検討した、情報セキュリティ未来予想図Ⅲに触れられている「セキュリティ意識しない究極セキュリティ＝普遍的（Universal）セキュリティ環境」が将来的な 安全・安心 EC 基盤のベースとなるものであり、その実現のための技術的な KEY WORD として下記の項目を挙げておくものとする。

- 検疫ネットワーク＝操作端末～LAN まで入込めないウイルス（隔離・治療）
- ハニーポット（擬似ノンセキュリティ環境）へのマルウェア誘導システム
- マルウェア自動解析システム（格納・解析・レポート・駆除ツール・監視）
- エージェントからネットワーク管理者・EC 端末操作者に対する侵入パターン
  分析・対策＆結果レポート
- セキュリティ・インシデント分析システム（ネットワーク＆端末レベル＆各相関）
- 統合認証基盤（本人認証）のしくみ（ID 管理と電子証明書）
- マルウェア（悪意）全般対応、複合的（階層的）アクティブセキュリティシステム
  （回線提供+サービス提供+オフィス・ホーム<ラスワン内>各サーバー複合検疫 S）

つまり、これらこそが本当の意味での、能動的（Active）セキュリティシステム構築であり、来年度以降 ECOM 情報セキュリティ WG 活動としては、今年度各サブワーキングテーマの将来的な取り組みに加えて、このテクニカルな対策を実現する「共通バイブル（拠り所となる各種ガイドライン等）」の策定も視野にいれて活動していきたい。
さらに、今後の活動の大きな柱としては上記のような、従来型発想である情報保護するためのセキュリティ保護から、今年 SWG1 で取上げた「情報利活用や情報共有に向けたセキュリティ（例：業務プロセスセキュリティ評価チャート＝BPS‐EC）」のような新しい観点での取り組みを行っていきたいと思っている。
この評価チャートは、アウトソーシング業務や開発コラボレーション業務に関する、情報セキュリティ作業の確認ツールの位置づけであり、これが標準化され普及することは各企業にとってもプラスになると考えられ、さらにビジュアル化という点で企業の海外展開にも活用できるものと想定できる。
このような新しい発想に立った、情報利活用のためのセキュリティ保護という視点でのワーキング活動展開も次年度より検討・実施したいと考えている。

以　上

EC における情報セキュリティに関する活動報告書 2008

平成 21 年 3 月　発行

発　行　　次世代電子商取引推進協議会

販　売　　財団法人　日本情報処理開発協会
電子商取引推進センター
東京都港区芝公園 3 丁目 5 番 8 号
機械振興会館 3 階
TEL:03（3436）7500

この資料は再生紙を使用しています。

ISBN978-4-89078-674-9 C2055